Security Testing Report

EDI\Interoperability Solutions

XDS 2023-2

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Table of Contents

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Document Version Control

Name of the document : XDS 2023-2 Security Testing Report			
Version: 8.0	**Intake ID:**	2764	
Document Definition: This document highlights the vulnerabilities currently existing in the application under scope. It also documents possible actions to be taken to reduce/eliminate vulnerabilities.	**Document ID:**	PRHC/C40/SVN/87857	
Author: Sai Praneetha Bhaskaruni, Harshal Kukade	**Effective Date:**	25/Oct/2023	
Reviewed by: Chaitra N Shivayogimath			

Document History

Version	Date	Author	Section	Changes
0.1	20/Jul/2020	Narendra Makkena	Complete	Initial Draft
1.0	20/Jul/2020	Taksh Medhavi	Complete	Addition & review
1.1	01/Mar/2021	Shabana Bagum	Complete	Initial Draft
1.2	02/Mar/2021	K K Ashwin	Complete	Addition & review
2.0	03/Mar/2021	Narendra Makkena	Complete	Final review
2.1	03/March/2022	Shibija K	Complete	Initial Draft
2.2	04/March/2022	K K Ashwin	Complete	Addition & review
3.0	04/March/2022	Pranati Mohanty	Complete	Final review

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

3.1	27/May/2022	Sreerag M	Vuln 8.2,8.4,8.6 and 8.11	Retest
3.2	27/May/2022	Shibija K	Vuln 8.2,8.4,8.6 and 8.11	Addition & review
4.0	27/May/2022	Pranati Mohanty	Vuln 8.2,8.4,8.6 and 8.11	Final Review
4.1	27/Aug/2022	Kartik Lalan	Complete	Addition & review
5.0	29/Aug/2022	Shibija K	Complete	Final Review
5.1	31/Jan/2023	Ashwin K K	Vuln 8.2,8.4,8.6 and 8.11	New feaure and retest
5.2	01/Feb/2023	Shibija K	Complete	Addition & technical review
6.0	01/ Feb /2023	Pranati Mohanty	Complete	Final Review
6.1	08/Jun/2023	Raj Kiran Rudrapati	Complete	Issue revalidation & Rapid test
7.0	09/Jun/2023	Aravind C Ajayan	Complete	Addition & Review
7.1	25/Oct/2023	Sai Praneetha Bhaskaruni, Harshal Kukade	Complete	Addition & Retest
8.0	25/Oct/2023	Chaitra N Shivayogimath	Complete	Final Review

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Distribution List

User/Department/Stakeholder	E-Mail ID
Project Owner and PSO	subhash.naga@philips.com; Stephanie.Heidstra@philips.com; moin.creemers@philips.com; ManishKumar.MachingalSukumar@philips.com; Stephanie.Heidstra@philips.com; chidamber.kumar_1@philips.com; abhishek.kumar.pathak@philips.com; revathi.r@philips.com

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

1. Definitions & Abbreviations

Term	Explanation
SCoE	Security Center of Excellence
TLS	Transport Layer Security
SSL	Secure Socket Layer
XSS	Cross Site Scripting

The severity of every vulnerability has been calculated by using industry standard **Common Vulnerability Scoring System (CVSS)** used for assessing the severity of computer system vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score (Scores range from 0 to 10, with 10 being the most severe) reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organization properly assess and prioritize their vulnerability management processes.

The severity rating for the numerical values are mapped below:

None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

The **Severity** and **CVSS vector** of each vulnerability is calculated using the CVSS V3 **Base Score Metrics** Calculator located here. Vulnerabilities identified during security assessment are classified into standardized categories. Refer following table for more information:

Categories for vulnerability classification

Web application security assessment	OWASP Top Ten - 2021
Mobile application security assessment	OWASP Top Ten - 2016
IoT/Hardware security assessment	OWASP Top Ten – 2014

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

2. System Details & Architecture

Brief about the product architecture:

Philips Interoperability Solutions (formerly Forcare) is an open-standard-based interoperability software solutions for fast and flawless data flows between medical systems and information sources at the departmental and enterprise levels, as well as Health Information Exchanges (HIEs) across health systems.

The tested components: ForView, ForAudit ForImageUpload and ForAdmin web application.

ForAdmin - ForAdmin is a web-based application for system administrators. This can be used for configuring and monitoring the Forcare application components in your network. With ForAdmin, you can make configuration changes at runtime without requiring restarting your server. Component configurations are stored in XML files that are validated to prevent basic configuration errors.

ForView- ForView is an application for care providers that lets them find, view, and share patient-oriented clinical information. ForView complements existing clinical information systems, adding the ability to view documents and images from a variety of sources that are not limited to one specific institution or document type.

ForAudit- ForAudit is an IHE ATNA Audit Repository. It captures audit logs sent via UDP or TCP/SSL (syslog, per IHE ITI ATNA) and supports HTTP or HTTPS based audit transactions.

ForImageUpload- ForImageUpload is an application to upload Dicom/Zip files of images.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

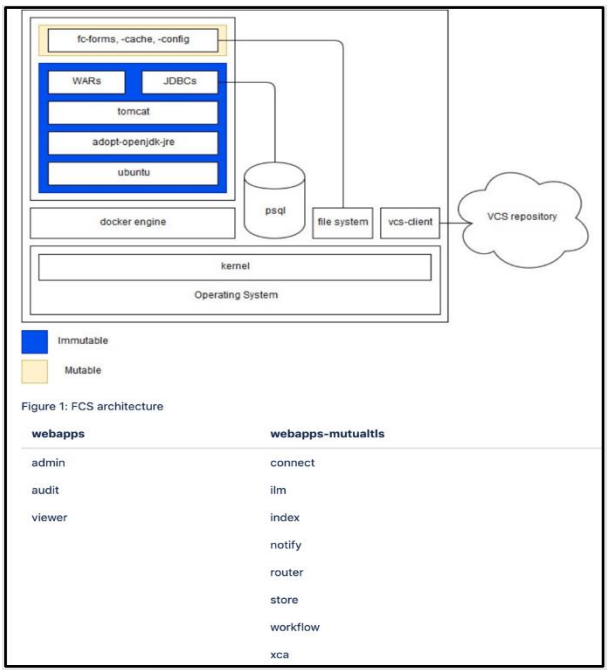


Figure 1: FCS architecture

webapps	webapps-mutualtls
admin	connect
audit	ilm
viewer	index
	notify
	router
	store
	workflow
	xca

The environment provided for security testing is a Pentest Environment.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

3. Scope

The scope of this security assessment is to perform **Grey box** security testing to find security threats that may come from a malicious outsider or insider user of the **XDS 2023-2.** Security testing on **Web applications (Viewer, Audit, Admin, & ImageUpload)** of **XDS 2023-2** is performed.

The following list includes some examples of major activities performed during the assessment:

Web Application:

- Crawl through complete scope of the web application/service space and identify for any unauthenticated URL or directory.
- Check for all input injection-based attacks across all the possible entry fields in Web API.
- Exploiting any known component vulnerability or service misconfiguration.
- Reviewing the transport layer security implemented.

*Follow "*Test case execution*" section to get the detailed about test*

Type	Scope of Assessment		
Web Application	XDS 2023-2	URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload/
		Version	2023-2
		Environment	Pentest
		User Roles	root (Self Creatable User Roles)

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

4. Out of Scope

Below mentioned items are out of scope for the current security assessment:

- Source code review
- Cloud Testing
- Docker Testing
- Complete security assessment of 4 portals

Note: We have covered the testing of **XDS 2023-2** in the environment provided and the results are valid if the same environment is replicated. Re-run the tests if a new propagation of the environment is made.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

5. Executive Summary

Security Center of Excellence (SCoE) team is engaged in activities to conduct security assessment of **XDS 2023-2** which included **Web applications** in scope. The purpose of the engagement is to evaluate the security of the **XDS 2023-2** against industry best practice criteria.

Note: Only highlights of important vulnerabilities are described below. Please refer 'Vulnerability Summary' section for complete detailed list of vulnerabilities.

During the security assessment following factors are found with consideration for significant improvement:

- Using known vulnerable components
- Broken Access Control
- Security Misconfigurations

During the security assessment of the product, security issues in the below areas are not found:

- Injection attacks

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

VULNERABILITY SUMMARY CHART

The graph below shows a summary of the number of vulnerabilities and their severities.

Note: The vulnerabilities mentioned in this report are technical vulnerabilities only. The Product Security Risk Assessment would report the business risks associated with these vulnerabilities.

Critical	High	Medium	Low
0	0	3	8

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

6. Vulnerability Summary

The findings and vulnerabilities from the assessment are explained in the below table:

Finding No.	Vulnerability Title	Technical Risk	Impacted Area	CVE ID*	Status	Status (23-Oct-23)
30132	Using Known vulnerable components	Medium	Webapp	Refer 8.1	Open	Open
79143	Broken Access Control	Medium	Webapp	NA	Open	Open
30136	Weak Password Policy	Medium	Webapp	NA	Open	Open
77505	DOM Cross Site Scripting	Low	Webapp	NA	Open	CLOSED
30145	Weak Input Validation	Low	Webapp	NA	Open	Open
30209	Improper error & exception handling	Low	Webapp	NA	Open	Open
37688	Sensitive information in the URL	Low	Webapp	NA	Open	Open
30128	HTTP Strict Transport Security (HSTS) Not Implemented	Low	Webapp	NA	Open	Open
30146	No Account Lockout Policy	Low	Webapp	NA	Open	Open
30125	Reflected Cross-Site Scripting (XSS)	Low	Webapp	NA	Open	CLOSED

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

83850	Weak SSL/TLS Configuration	Low	Webapp	NA	Open	Open
88944	Missing Security Header	Low	Webapp	NA	-	Open
88946	Server Banner Disclosure	Low	Webapp	NA	-	Open

*CVE ID are mentioned for the vulnerabilities which has a known external CVE.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7. Observations

Below mentioned observations are not considered as vulnerability but informative to the business.

Observations which shows good implementation or best practice identified:

- XSS protection flag is enabled.

Request

Pretty Raw Hex

```
GET /viewer/services/domain/list.json HTTP/2
Host: ec2-3-71-200-223.eu-central-1.compute.amazonaws.com
Cookie: JSESSIONID=58BCA220735453D8096B54F32AC7DC27
Sec-Ch-Ua:
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/115.0.5790.110 Safari/537.36
Sec-Ch-Ua-Platform: ""
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient/query.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Content-Type: application/json;charset=UTF-8
Date: Sat, 21 Oct 2023 10:38:36 GMT
Expires: 0
Forcare.com-Logcontext: 79a8f001e495/viewer-24272
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 329

{
  "identifier":"id",
  "allowPatientIdQueryWithoutDomain":false,
  "targetDomain":"",
  "items":[
    {
      "id":"1.3.6.1.4.1.21367.2005.3.8",
      "name":"Hospital",
      "shortName":"HOS"
    },
    {
      "id":"1.3.6.1.4.1.21367.2005.3.7",
      "name":"IntelliSpace Exhange",
      "shortName":"ISX"
    },
    {
      "id":"2.16.840.1.113883.2.1.4.1",
      "name":"Citizen Service Number",
      "shortName":"BSN"
    }
  ]
}
```

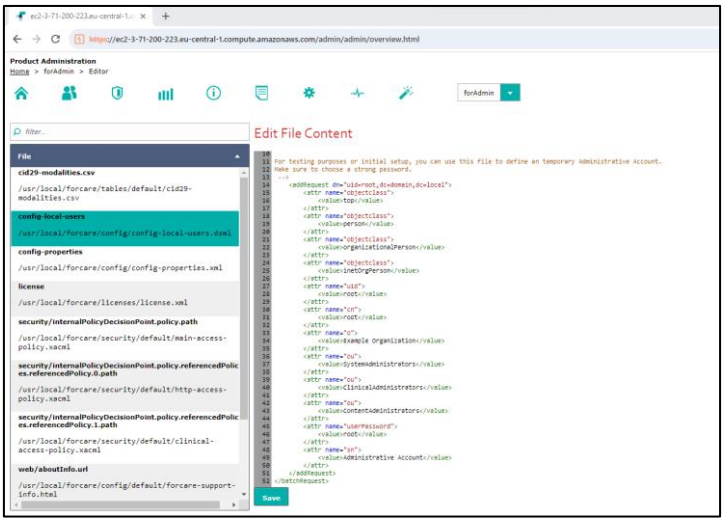
- The usage of the required HTTP methods has been defined properly at the server end. Which means if a GET request is used and if a different request is tried, then the server responds with “405” method not allowed error which is a good observation.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

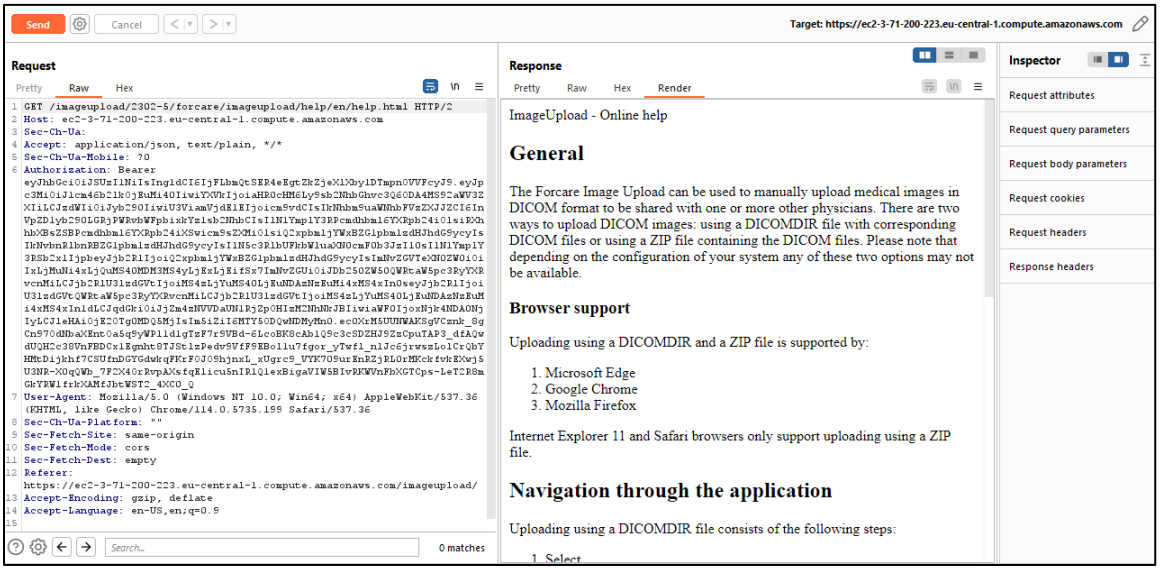
Printed copies are uncontrolled unless authenticated.

Observations which shows missing best practice or possible weak implementation (this may/may not be direct active threat):

- No email verification while registering the user.
- Application allows simultaneous session logons.
- Password is in plain text at admin portal in the configurations.



- ImageUpload Online help page does not require any authentication. Since there is no PII or PHI we are marking this as Observation.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8. Detailed Vulnerability Report

8.1 Webapp: Using Known Vulnerable Components

Vulnerability Title	Using Known Vulnerable Components
Vulnerability Category	A6 Vulnerable and Outdated Components
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 4.8 CVSS:3.0/ AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
Description	**Vulnerability Description:** During the security assessment of the product, it is observed that the web application is using components with known vulnerabilities and associated CVEs. Technologies are like jquery-1.2.6, dojo 1.9.6 and AngularJS v1.8.2 have known CVE IDs: jquery-1.2.6, AngularJS v1.8.2, and dojo 1.9.6 • moment.js 2.29.3 - CVE-2022-31129 • jquery-1.2.6 - https://nvd.nist.gov/vuln/detail/CVE-2011-4969 • AngularJS v1.8.2 - angular 1.8.2 vulnerabilities | Snyk • Dojo 1.9.6 - https://security.snyk.io/package/npm/dojo/1.9.2 AngularJS LTS discontinued. Discontinued Long Term Support for AngularJS | by Mark Thompson (@marktechson) | Angular Blog **Retest (23-October-2023)**: All the mentioned vulnerable components are still present in this application. **Exploitability Rational:** Published vulnerabilities have a greater likelihood of exploitation by attackers due to readily available proof-of-concept code that exploits the issue or integrates the exploits into freely available testing tools. **Impact Rational:** Depending on the nature of known vulnerabilities, this can allow an attacker to compromise the server and any data stored within.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit
Recommendation	Service version is vulnerable to an attack, take preventative measures to mitigate the vulnerability until an upgrade or patch is released.
Status	**OPEN**

Steps to Reproduce:

Retested (23rd October 2023):

Steps to Reproduce:

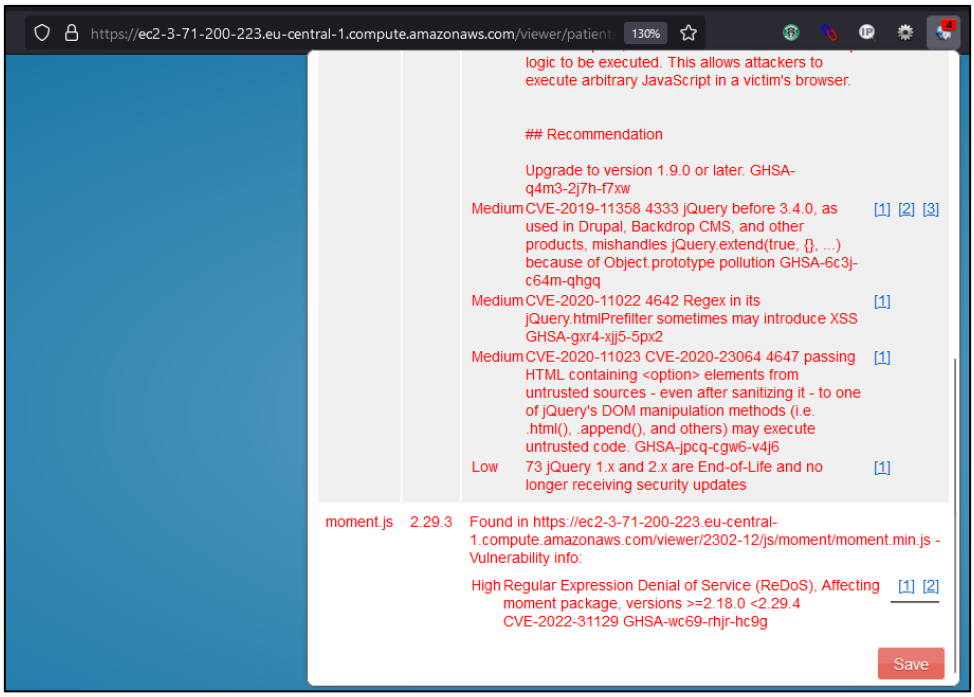
- Launch the application and run retire.js plugin.
- Login to any application ForAdmin, ForView, ForAudit.

Supported Evidences:

For View Portal:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



For Admin Portal:

For Audit Portal:

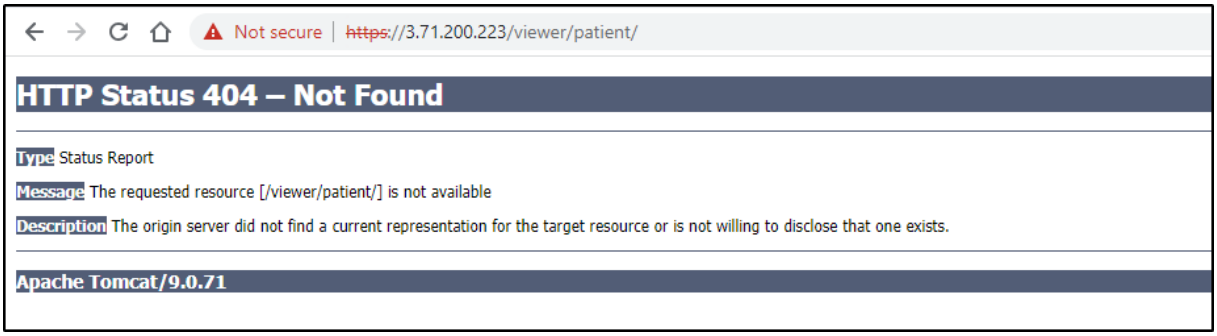
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Steps same as before

audit_login_pg_only.html

viewer_retirejs.html



Old POC:

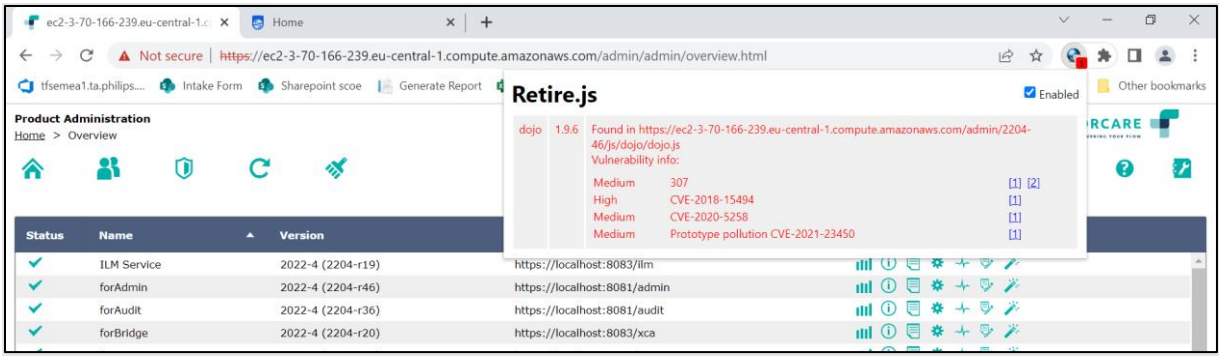
- Launch the application and run retire.js plugin.
- Login to any application ForAdmin, ForView.

ForView Portal

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

ForAdmin portal



Banner grabbing of Apache Tomcat server version.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.2 Webapp: Broken Access Control

Vulnerability Title	Broken Access Control
Vulnerability Category	A1 Broken Access Control
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 6.5 CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Description	**Vulnerability Description:** The application allows lower privileged users to access resources or perform actions which is available to a higher-level account. This usually occurs when the server does not perform authorization/entitlement checks on each request to ensure that the user has the appropriate privileges before executing the request, or when those checks are made based on values that can be tampered with on the client-side. It is observed that the user without SYSTEM_PHI_READ role defind can view/read the following API endpoints which consists of sensitive information like, backend components/versions, encryption password etc. **Retest (23-Oct-2023)**: It is observed that user with SYSTEM_PHI_READ has view option on backend configuration which includes sensitive information. Issue still persists. **Exploitability Rational:** The attacker can be any user who has access to the forcare admin application. **Impact Rational:** Depending on the nature of the information, a malicious user may obtain personally identifiable information (PII), private user data or information which can allow user impersonation (in the event of credential or session identifier).
Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/services/admin/components/viewer/config/properties.json

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	Note: This is an application wide issue. Instances are not limited to the above items. Fix should be applied across the platform.
Recommendation	Check and verify the privileges of the user and check or verify before serving the response.
Status	**OPEN**

Steps to Reproduce:

Retest (23-Oct-2023):

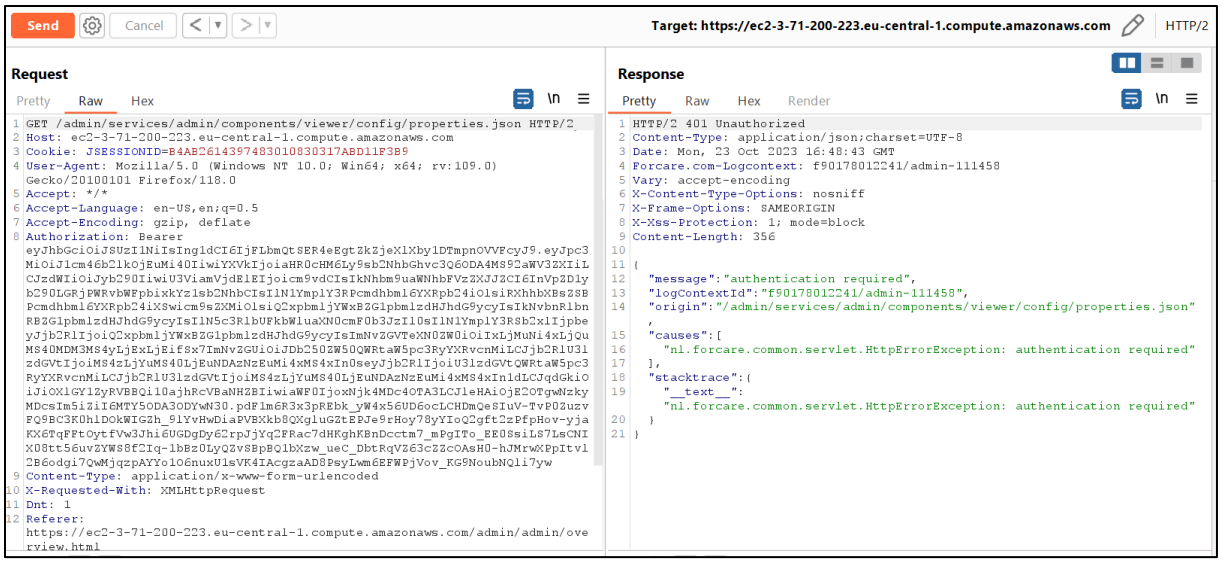
Case 1:

Step1: Configure the browser with a proxy tool like Burp Suite and log into the foradmin application.

Step2: Leave the setup idle for about 5-10mins, the token becomes unauthorized.

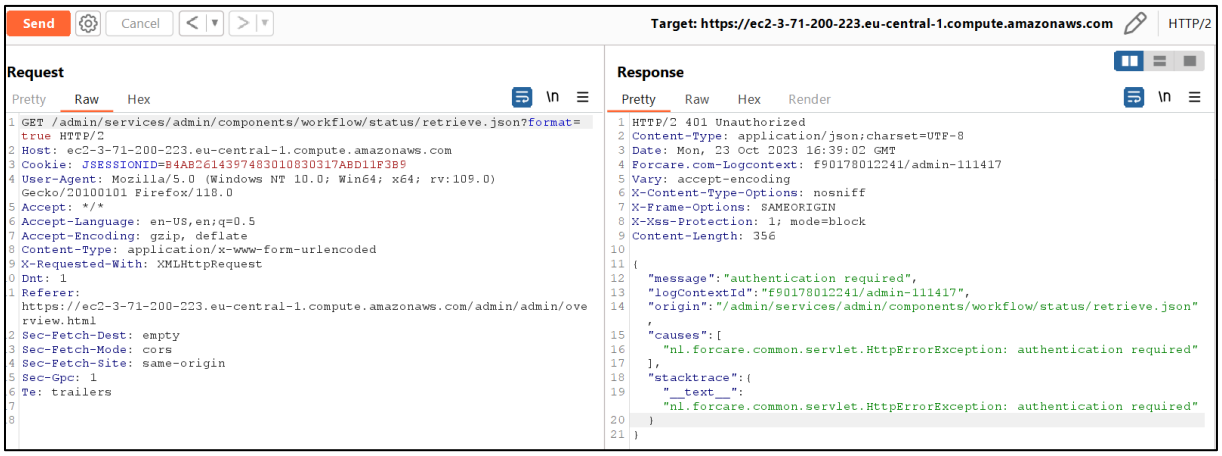
Step3: Send the retrieve data request to repeater and observe the behavior.

Supported Evidences:



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Once the Token is expired, when we send the retrive.json request that also gives the 401 unauthorized error message, hence this case 1 is fixed.

Case 2:

Step1: Configure the browser with a proxy tool like Burp Suite and log into the foradmin application.

Step2: Capture this request(https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/services/admin/components/admin/config/properties.json) and send to repeater

Step3: Logout from Admin account

Step4: Now capture the cookies and tokens of Viewer and Audit account replace with admin cookies and tokens and forward the request

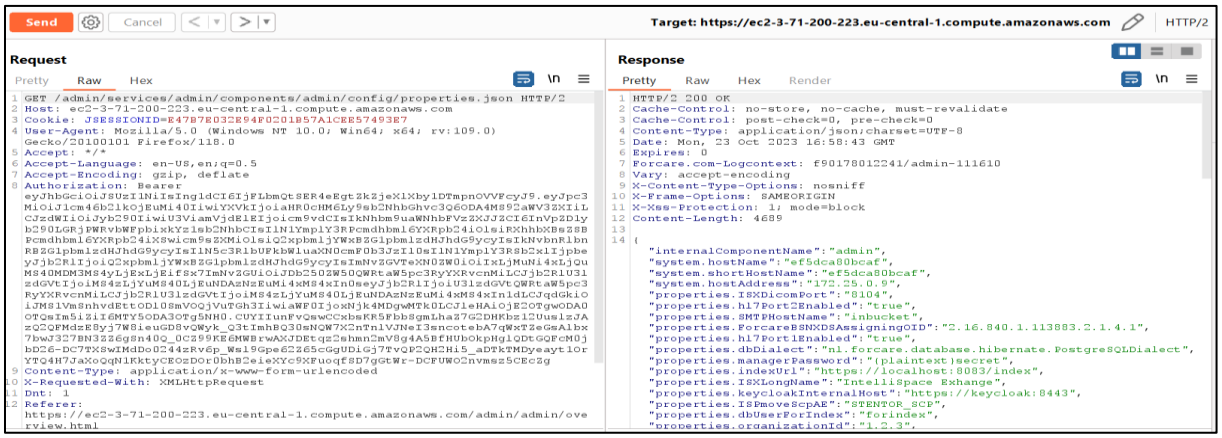
Step5: You can see that Viewer and Audit users can view the admin properties.

Supported Evidences:

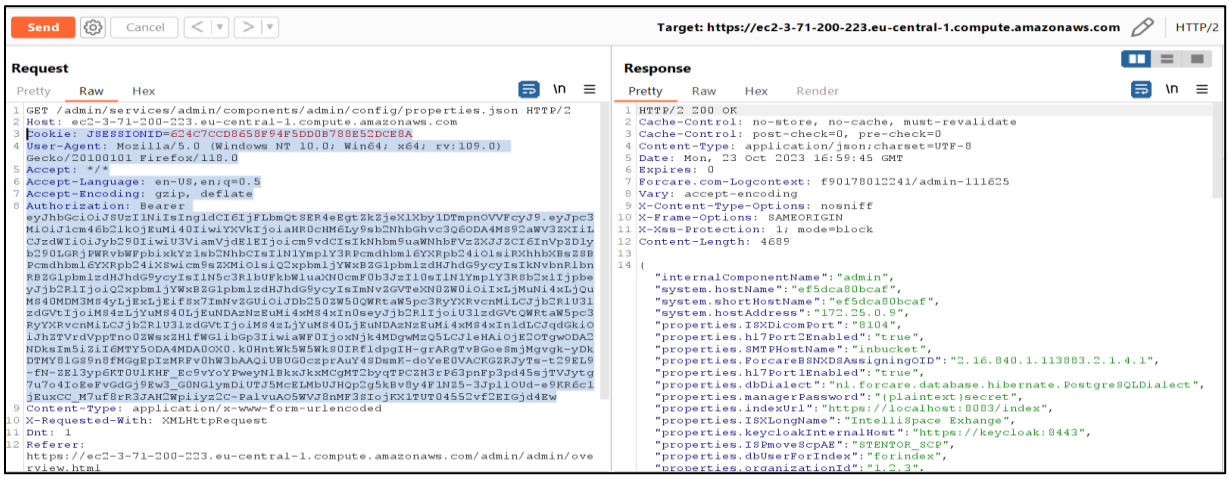
Actual request from Admin:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Modified request with Viewer and Audit cookies and tokens:



Retest (02-Jun-2023):

Case1:

The steps same as before

Case2:

Step1: Configure the browser with a proxy tool like Burp Suite and log into the foradmin application.

Step2: Leave the setup idle for about 5-10mins, the token becomes unauthorized.

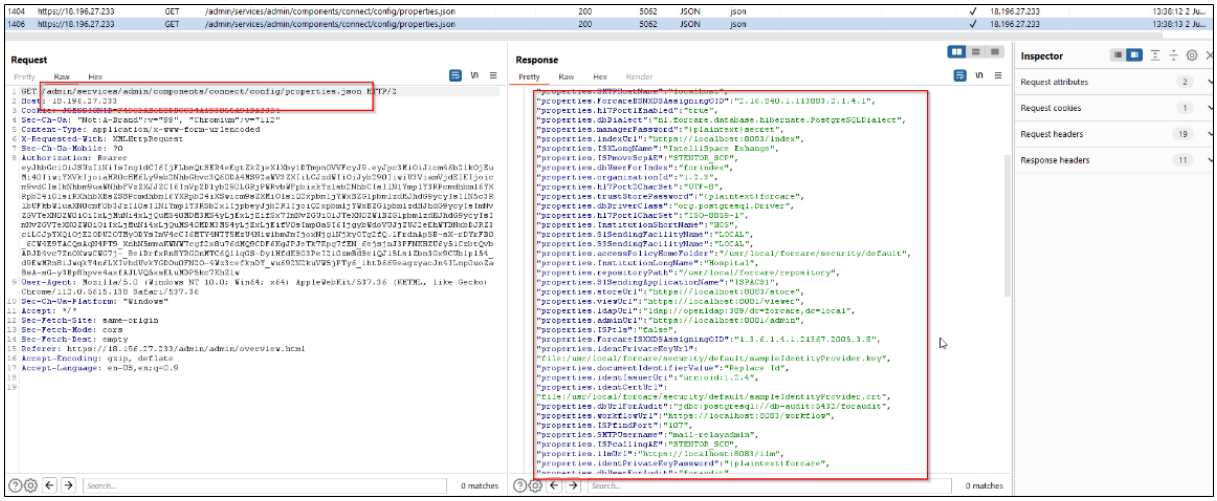
Step3: Send the retrieve data request to repeater and observe the behavior.

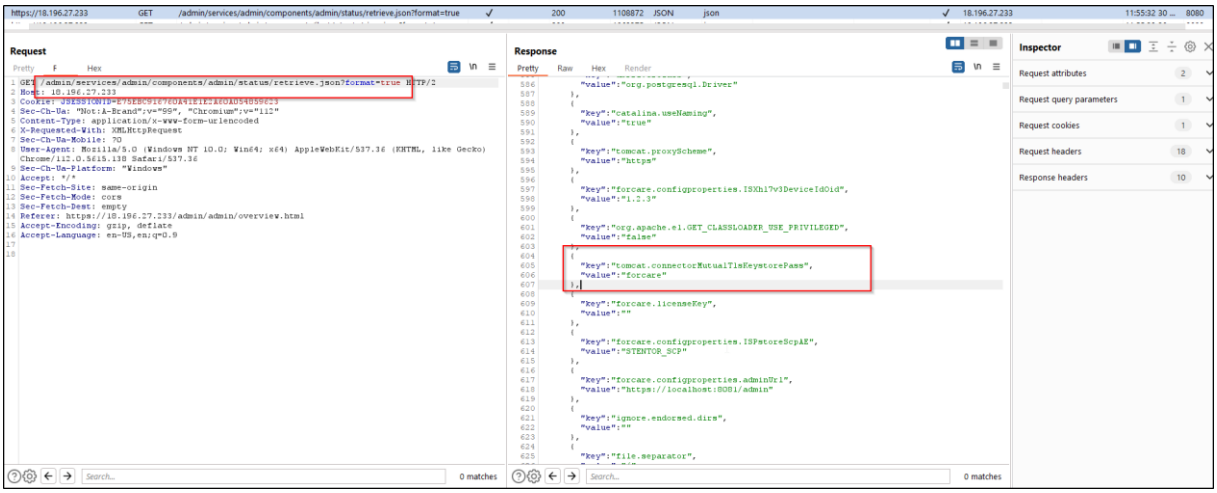
<u>Supportive Evidence:</u>

Case1:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

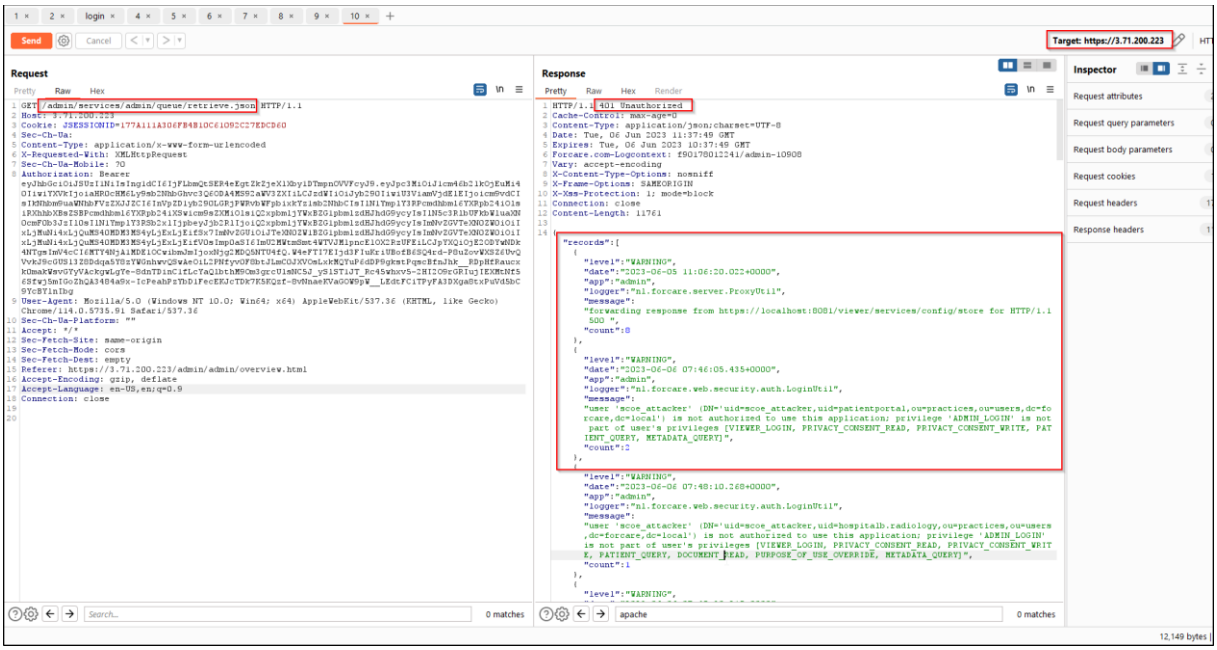




This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Case2:



Old POC:

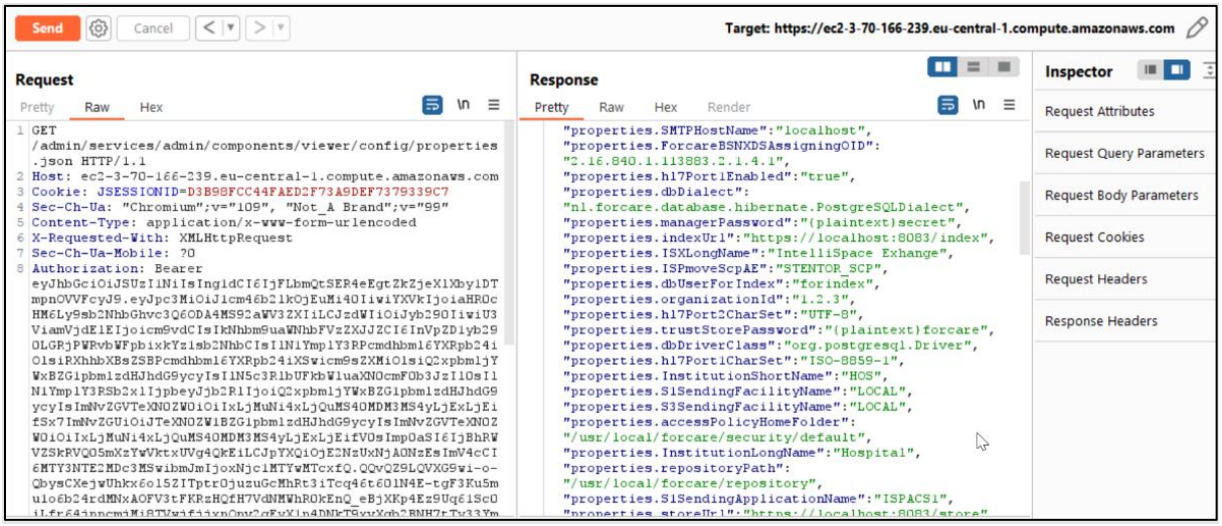
1. Configure your browser to use a proxy tool such as Burp.
2. Log in to the forcare admin application as user without SYSTEM_PHI_READ.
3. It is observed that the user without SYSTEM_PHI_READ role defined can view/read the following api endpoints which consists of sensitive information like, backend components/versions, encryption password etc.

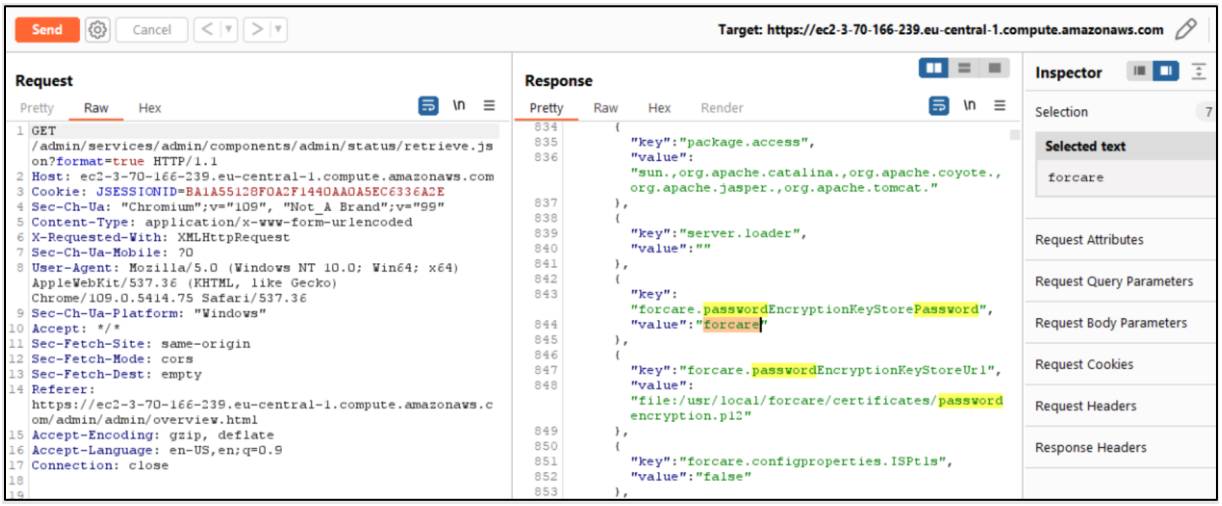
<u>Supportive Evidence:</u>

A user with SYSTEM_PHI_READ has view option on backend configuration which includes sensitive information.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.





This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.3 Webapp: Weak Password Policy

Vulnerability Title	Weak Password Policy
Vulnerability Category	A6 - Security Misconfiguration
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 4.6 CVSS:3.0/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:H/A:N
Description	**Vulnerability Description:** The application does not enforce a strong password policy to prevent malicious users from manually guessing or brute-forcing legitimate account passwords. Weak password policies include those that allow passwords consisting of common dictionary words, commonly-used passwords (For example., 1234), passwords that contain the associated username, sequential characters, and passwords shorter than 9 characters. By allowing users to create easily-guessable passwords, an attacker with minimal knowledge of registered users and username formats could crack passwords through the use of any of several techniques. In an online attack, an attacker can use consecutive login attempts to determine simple passwords. In an offline attack (For eaxmple., if the attacker has gained access to the raw contents of the password database through some other means), the attacker can employ richer techniques such as pre-computed hash attacks, free of rate-limiting and account-locking protections that might be employed against online password brute-forcing attacks. **Retest (23-Oct-2023):** Issue exists in retest, no password policy in place. **Exploitability rational:** Weak passwords may be easily guessed. This increases the likelihood a user's account may be compromised by an attacker. Once compromised, an attacker can have full access to the victim's account, potentially including the ability to modify settings, features and passwords. If the target account holds administrative privileges, the attacker can modify data for other users and/or the entire system. **Impact Rational:** Credentials can be easily brute force. . Due to the prevalence of password reuse, a compromised password may also provide an attacker with

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	credentials that can be used to attack other systems the victim uses the same credentials to access.
Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload
Recommendation	**Recommendation:** Implement a strong password complexity policy. A strong password policy is one which combines rules to prevent easily guessable passwords from being used while also ensuring that passwords contain sufficient entropy. A password policy which provides a large set of restrictions can ultimately result in a smaller potential pool of passwords, lowering the amount of time necessary to guess a password through brute-force attacks. Conversely, an overly permissive policy allows users to create easily guessable passwords. Put constraints in place to prevent users from choosing easily guessable passwords at the time of creation, specifically those that are targeted by well-known dictionary attacks. This can minimize the likelihood that an attack may be successful if an attacker attempts to guess commonly used passwords or employs an automated dictionary attack against a particular user. In the event that company policy does not stipulate password requirements, or the existing requirements are weak, consider employing the following password complexity requirements: • Passwords must be at least nine (9) characters long. • Passwords must contain some combination of at least three (3) of the following classes of characters: lowercase, uppercase, numeric, and “special” (For example., !, @, #, $, %, ^, etc.) characters. • Passwords should not be a dictionary word in any language, slang, dialect, jargon, etc. • Passwords should not be based on personal information, etc.
Status	**OPEN**

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Steps to Reproduce:

Retest (23-Oct-2023):

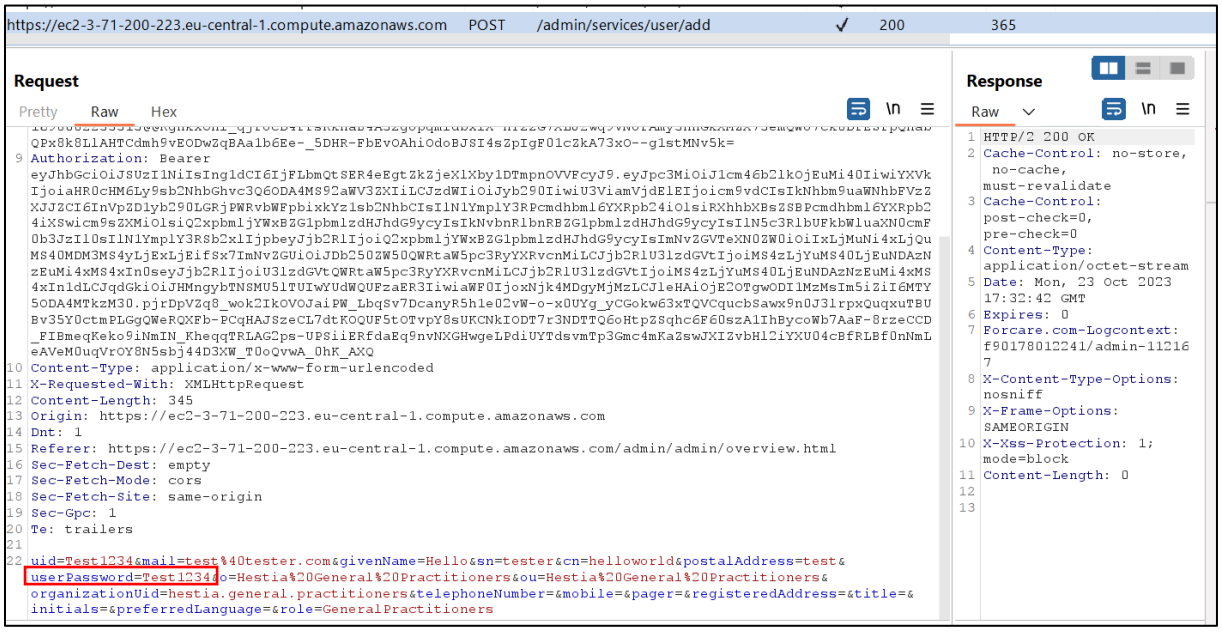
Steps to Reproduce:

Step1: Login to Admin account

Step2: Navigate to home -> User Management -> Users -> New User

Step3: Provide all the mandatory details (eg: im creating an account with Test1234/ Test1234 weak password)

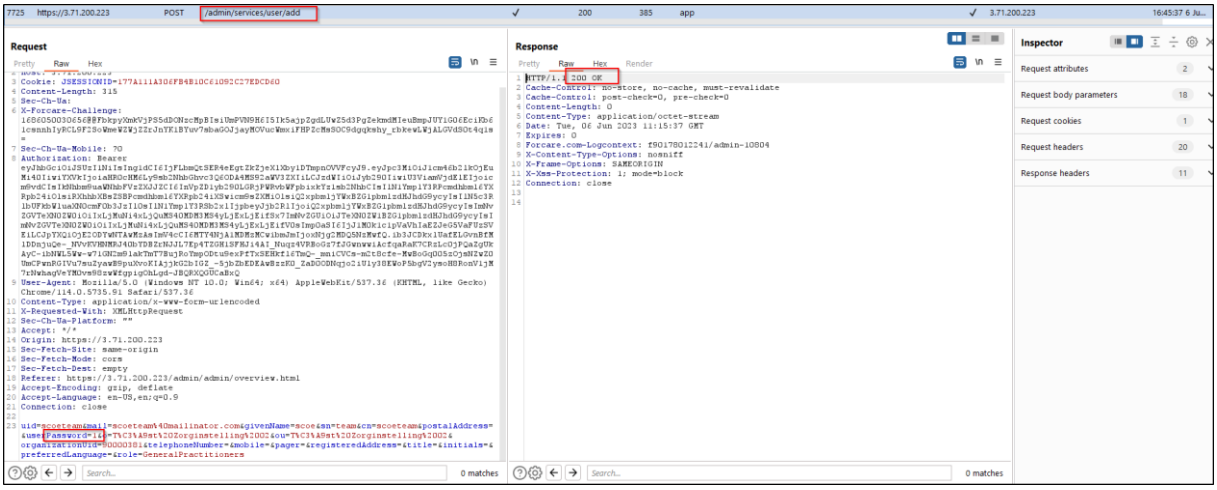
Supported Evidences:



Retest (05-Jun-2023):

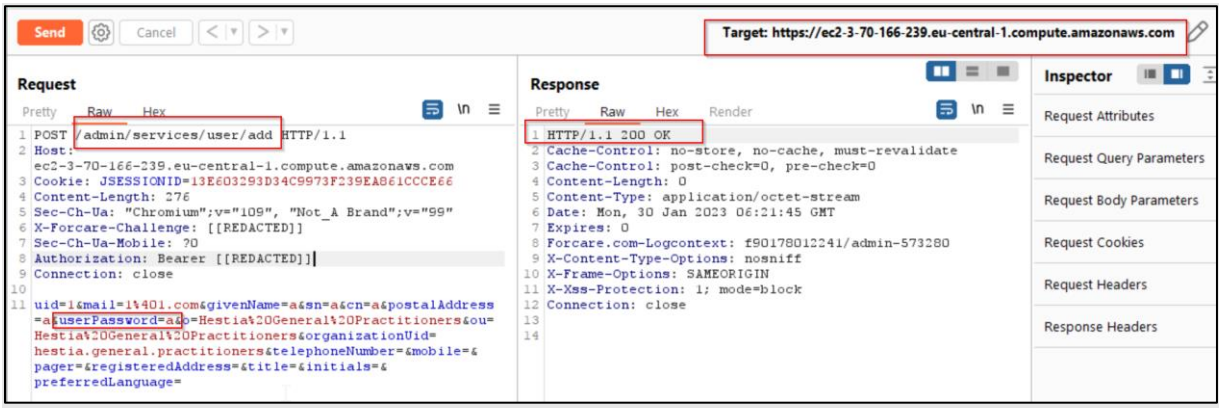
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

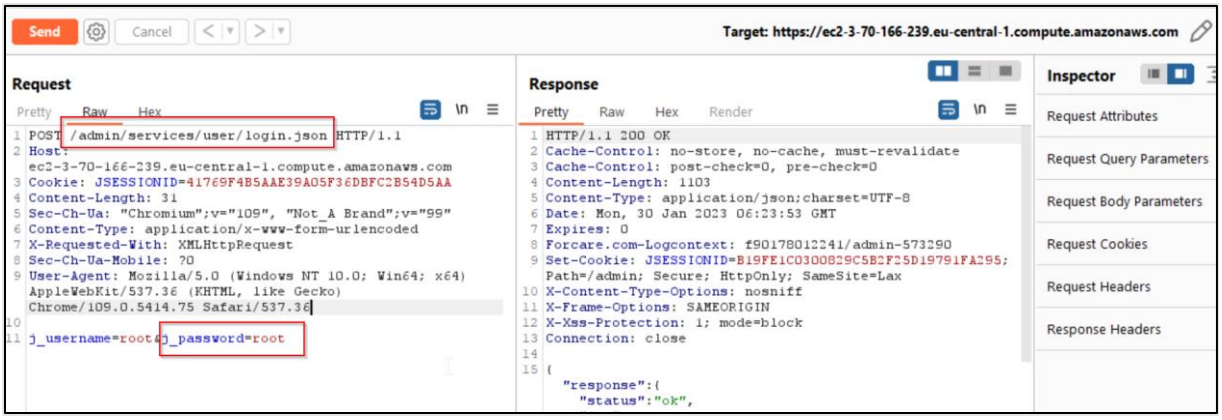


Old POC:

Weak password accepted for add user feature in ForAdmin portal.



Weak login password for the portals.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.4 Webapp: DOM Cross-Site Scripting (XSS)

Vulnerability Title	DOM Cross-Site Scripting (XSS)
Vulnerability Category	A3- Injection
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.5 CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** During the security assessment it is observed that the application is vulnerable to DOM XSS attack. DOM based XSS is an XSS attack wherein the attack payload is executed as a result of modifying the DOM "environment" in the victim's browser used by the original client-side script, so that the client-side code runs in an "unexpected" manner. That is, the page itself (the HTTP response that is) does not change, but the client-side code contained in the page executes differently due to the malicious modifications that have occurred in the DOM environment. **Retest (23-Oct-2023)**: Issue fixed in retest **Exploitability Rational:** For a successful exploitation of the issue, the victim should not be logged in to the application. **Impact Rational:** DOM Cross-Site Scripting vulnerabilities give the attacker control of HTML and JavaScript running the user's browser. The attack can alter page content with malicious HTML or JavaScript code. The attacker can arbitrarily alter page content displayed to the victim and can execute application functions using the victim's application identity if the victim is authenticated to the application.
Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient/query.html#/0/patient/query:_global!
Recommendation	It is recommended to have proper input validation, also checking syntax semantic (For example, a name field allowing special chars, number field accepting anything other than numeric digits., or allowing custom URL schema.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	Validation at Server side is required, you can bypass client side within JavaScript. Encode the output with Encoder.encodeForHTML and Encoder.encodeForJS before making dynamic updates to HTML. Considering any form of user input as untrusted and sanitizing it before operating anywhere. Avoid methods such as document.innerHTML and instead use safer functions, for example, document.innerText and document.textContent. If you can, entirely avoid using user input, especially if it affects DOM elements such as the document.url, the document.location, or the document.referrer.
Status	**CLOSED**

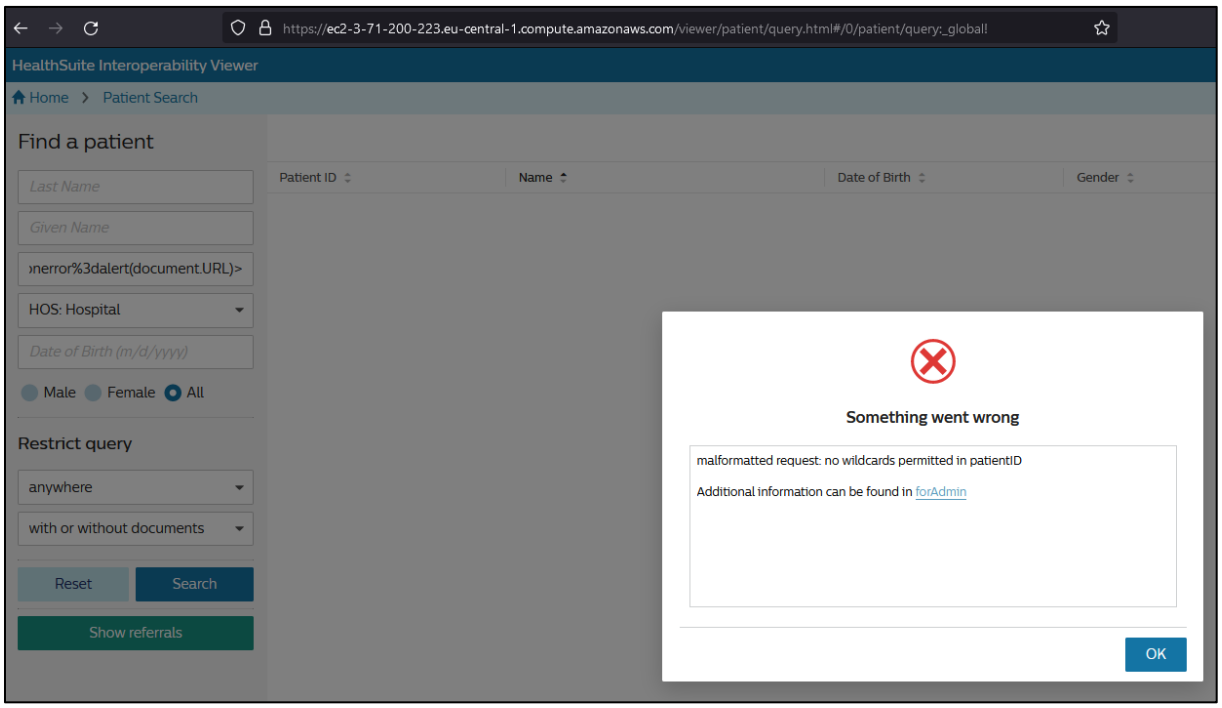
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Steps to Reproduce:

Retest (23-Oct-2023):

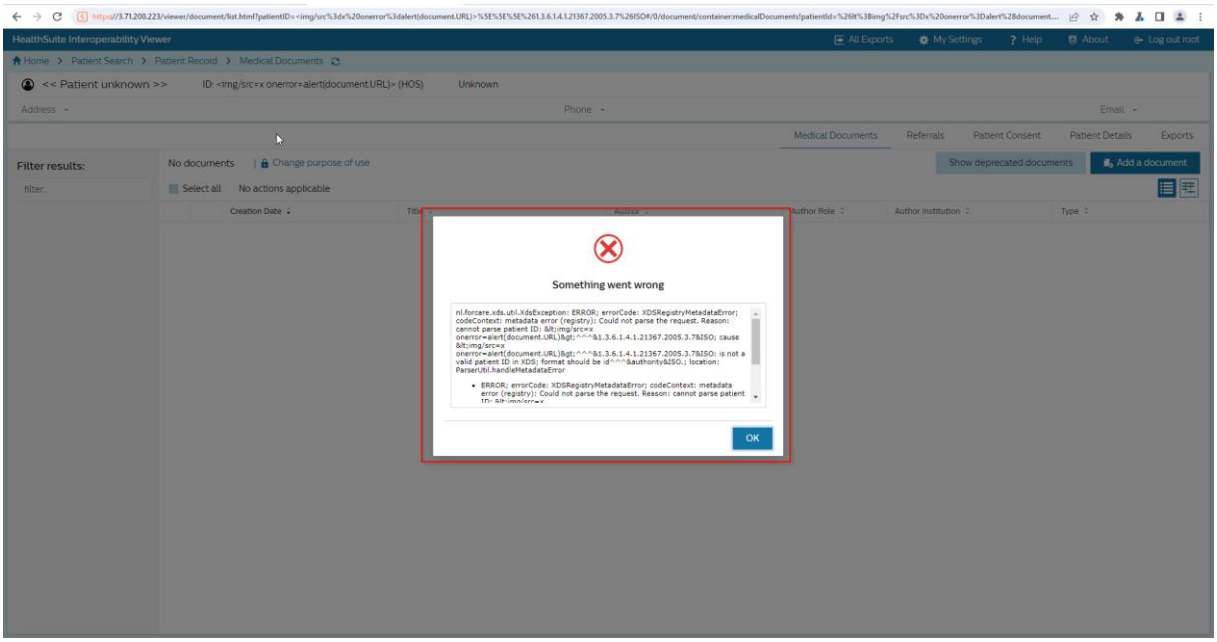
Supportive evidences:



Supportive evidences (03-Jun-2023):

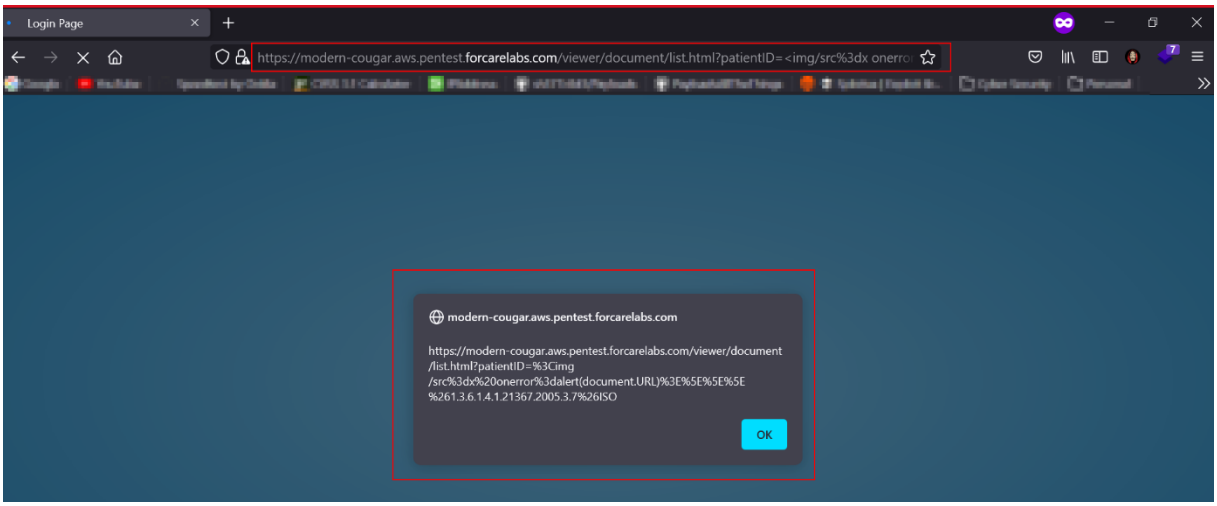
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Supportive evidences:

Payload: <img/src%3dx%20onerror%3dalert(document.URL)>

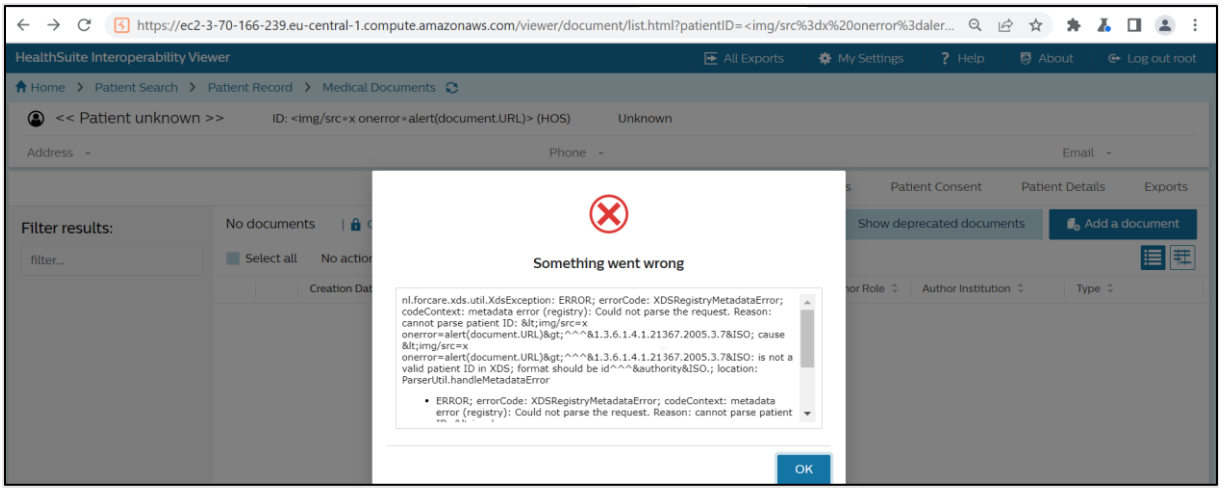


<u>Retest (31-Jan-2023):</u>

Throws uncaught exception error which indicates the fix is not implemented properly.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.5 Webapp: Weak Input Validation

Vulnerability Title	Weak Input Validation
Vulnerability Category	A3 - Injection
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L
Description	**Vulnerability Description:** During the assessment it is observed that the application stores or processes untrusted data that is not sufficiently validated. This may be due to a complete lack of validation or validation filters whose implementation does not provide sufficient protection for the given input. An application may obtain data from various external and internal sources including databases, file servers, web services, external client requests, etc. While some of these sources may be considered trustworthy, no assumptions should be made about the validity of data whose source cannot be explicitly verified. This includes not only external data, but also data that was previously stored by the same application and data generated by other entities in the same organization. **Retest (23-Oct-2023)**: Issue exists in retest. **Exploitability Rational:** Failure to properly validate and handle untrusted input represents the single largest category of software security weaknesses. At a minimum, data that is not validated may impact the application's control flow or data flow, leading to unexpected application states for end users, unintended changes to back-end data, as well as unexpected outcomes from executed application logic. An attacker may submit payloads that seek to exploit any number of vulnerabilities that typically result from a lack of input validation. These include (but are not limited to) SQL injection, cross-site scripting, LDAP injection, log injection, and command injection. The consequence of successfully exploiting these vulnerabilities varies, but most provide an attacker with the ability to bypass authentication and/or authorization mechanisms to access, modify or delete application and user data, or execute functionality only available to legitimate users. **Impact Rational:** An attacker can provide unexpected values and cause a program crash or excessive consumption of resources, such as memory and

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	CPU. An attacker can read confidential data if they can control resource references. An attacker can use malicious input to modify data or possibly alter control flow in unexpected ways, including arbitrary command execution.
Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer
Recommendation	We recommend the following: • Data that does not match an expected pattern and data that can potentially be used to execute injection attacks must be discarded or sanitized before use. • Perform the validation in such a way that end-users cannot tamper with or bypass the control. Perform the validation on the server-side rather than client-side. Whitelist validation should be favored first over other validation techniques since any character or string not explicitly specified as part of the "known-safe" set of characters or values is rejected or removed by default.
Status	**OPEN**

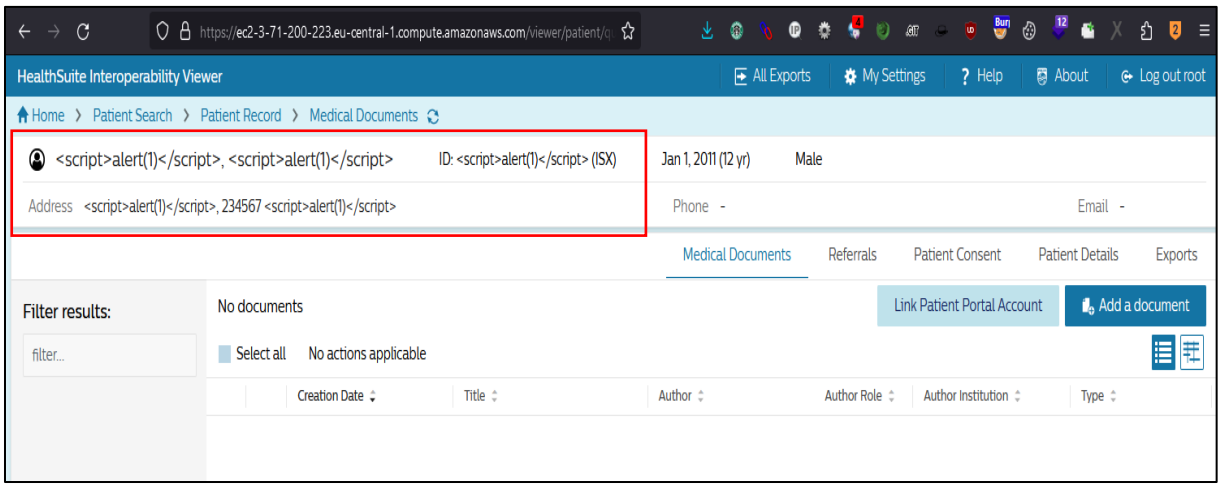
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

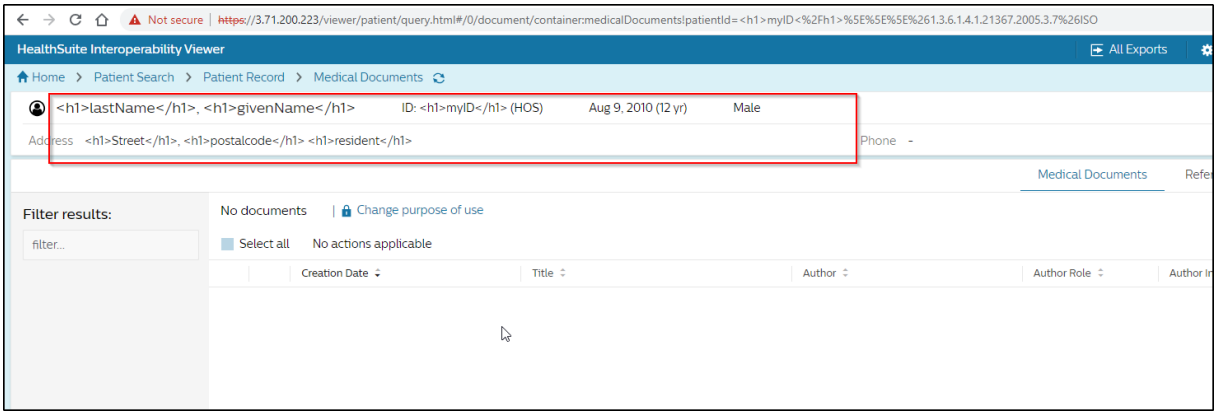
Steps to Reproduce:

Supportive evidence:

Retest (23-Oct-2023):



Retest (06-Jun-2023):



Old POC:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.6 Webapp: Improper Error & Exception Handling

Vulnerability Title	Improper Error & Exception Handling
Vulnerability Category	A6 - Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS v3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** it is observed that the web application reveals sensitive information as part of its error messages such as stack trace, server versions, name of server-side parameter. **Retest (23-Oct-2023)**: Issue exists in retest **Exploitability Rational:** An attacker does not require authentication to the platform in order to leverage this vulnerability. **Impact Rational:** Attackers may use this vulnerability to gain more information about the system before attempting to attack the web application.
Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit
Recommendation	It is recommended to Implement a mechanism to handle and log all errors that pull out the exception stack trace message. It is also recommended to display a generic error message instead of the stack trace.
Status	**Open**

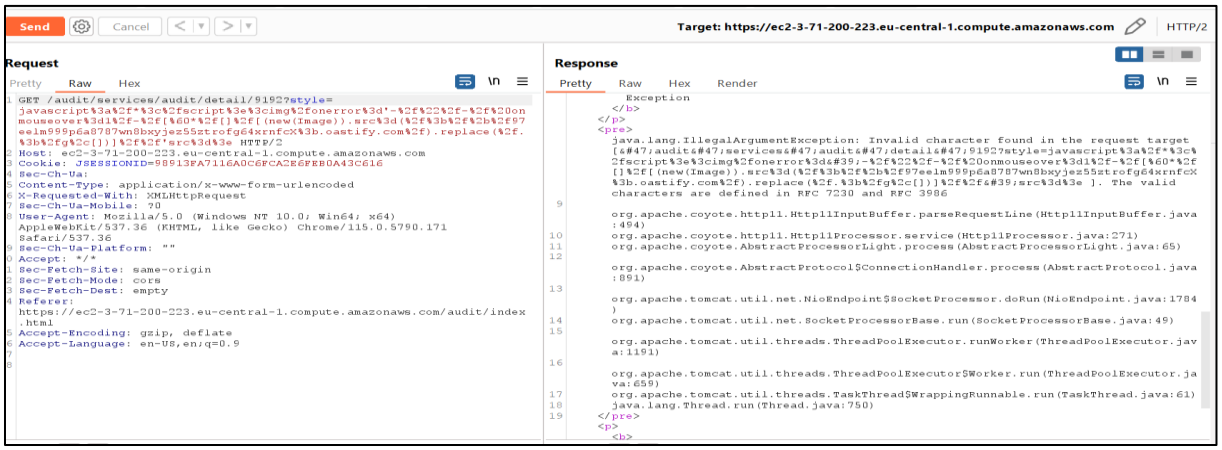
Steps to Reproduce:

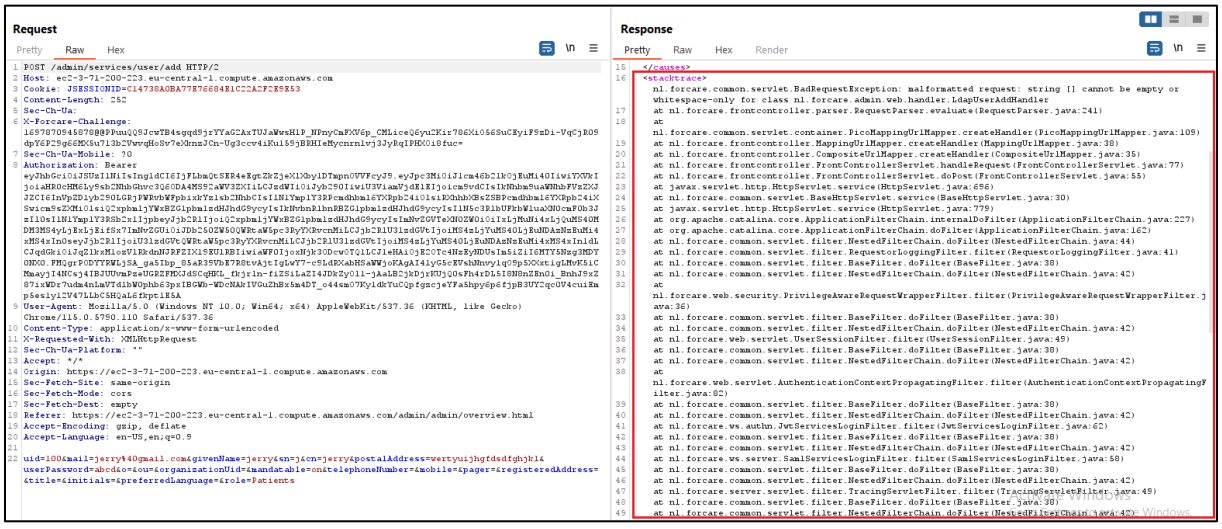
Retest (23-Oct-2023):

Supportive evidences:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

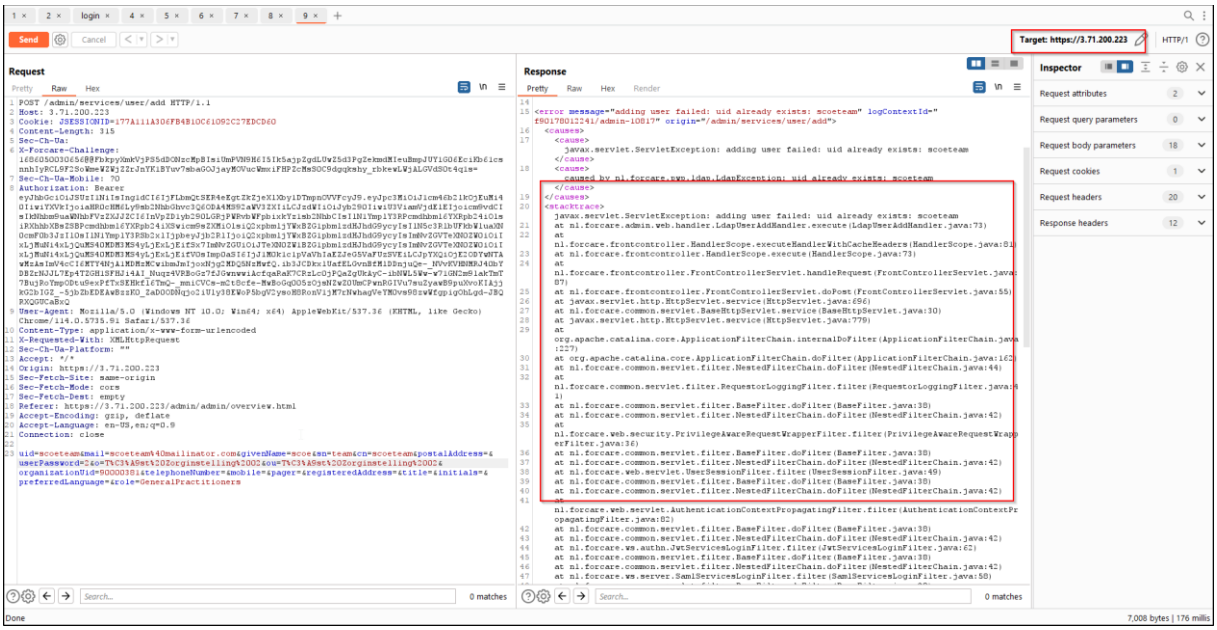




This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

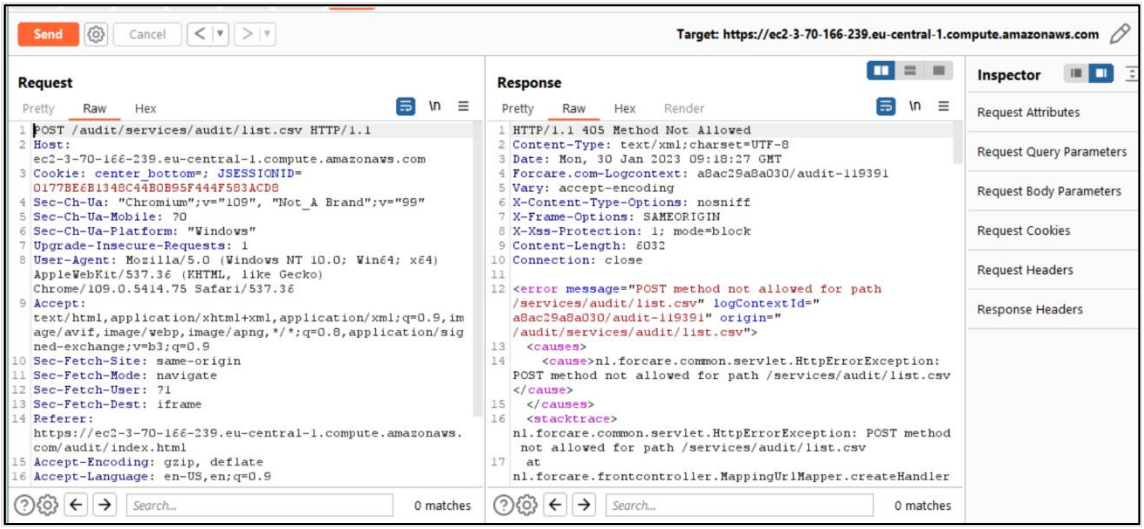
Printed copies are uncontrolled unless authenticated.

Retest (06-Jun-2023):



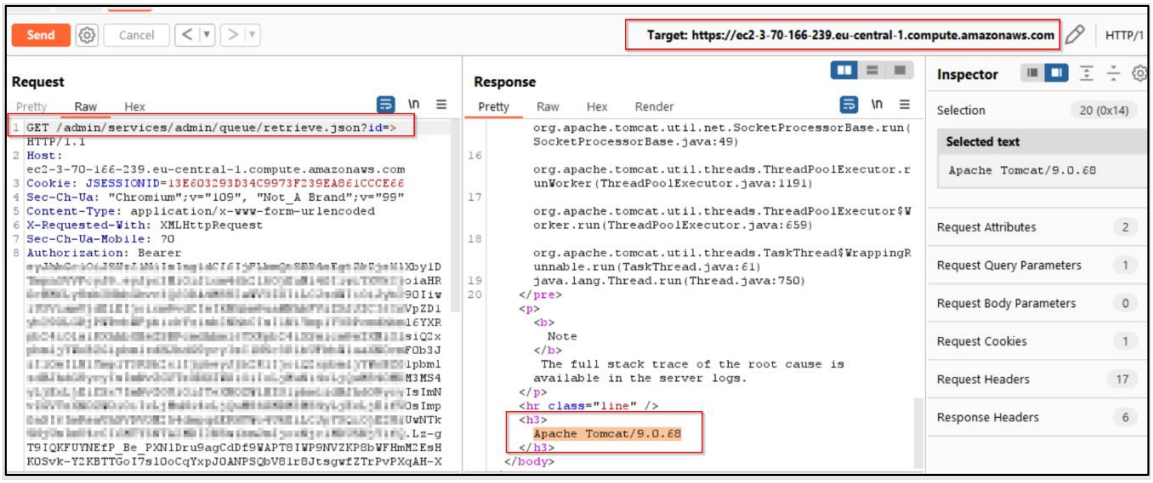
Old:

Improper error and exception as part of server response.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.7 Webapp: Sensitive Information in the URL

Vulnerability Title	Sensitive Information in the URL
Vulnerability Category	A6 - Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** During the security assessment, it is observed that Sensitive information is exposed in via URL query string parameters. Username, PatientID, userID, Code are exposed via URL parameters. URLs may be stored or viewed in multiple places during and after a request is made to the server: • URLs are often logged in multiple places including the browser history, proxy logs, and web server logs. • The query string will be sent as part of the URL if the URL is passed to another site via the Referrer header. • URLs sent to the user as part of an HTML page may be cached on disk. **Retest (23-Oct-2023)**: Issue exists in Retest. **Exploitability Rational:** Potential access vectors may include, but are not limited to: • Browser history, proxy logs, web server logs, etc. • Utilizing other attacks (such as cross-site scripting) to extract sensitive information from the source of a page containing links to URLs with sensitive information in the query string • Shoulder-surfing the URL in a user's browser address bar. **Impact Rational: A**ttacker who gains access to any location where URLs are stored can view sensitive information passed via the query string. Depending on the nature of the information, a malicious user may obtain personally identifiable information (PII), private user data or information which would allow user impersonation (in the event of credential or session identifier.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

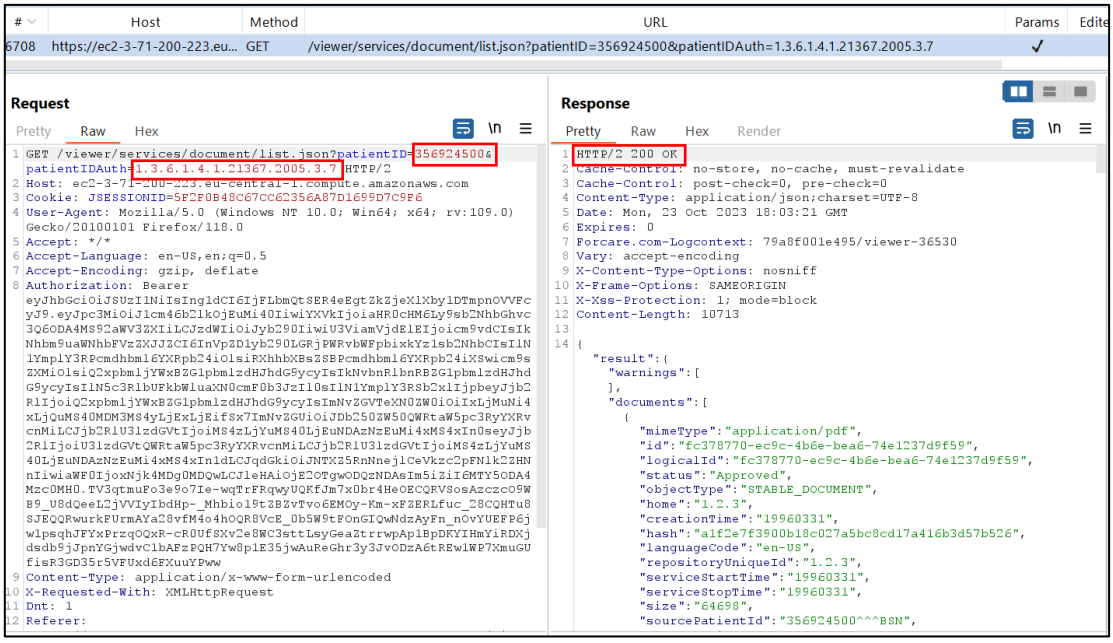
Printed copies are uncontrolled unless authenticated.

Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/services/document/list.json?patientID=356924500&patientIDAuth=1.3.6.1.4.1.21367.2005.3.7
Recommendation	Do not pass the sensitive data like credentials, UserID, codes or sessionIDs between the client and server via URL query string parameters.
Status	**OPEN**

Steps to Reproduce:

Retest (23-Oct-2023):

Supported evidences:

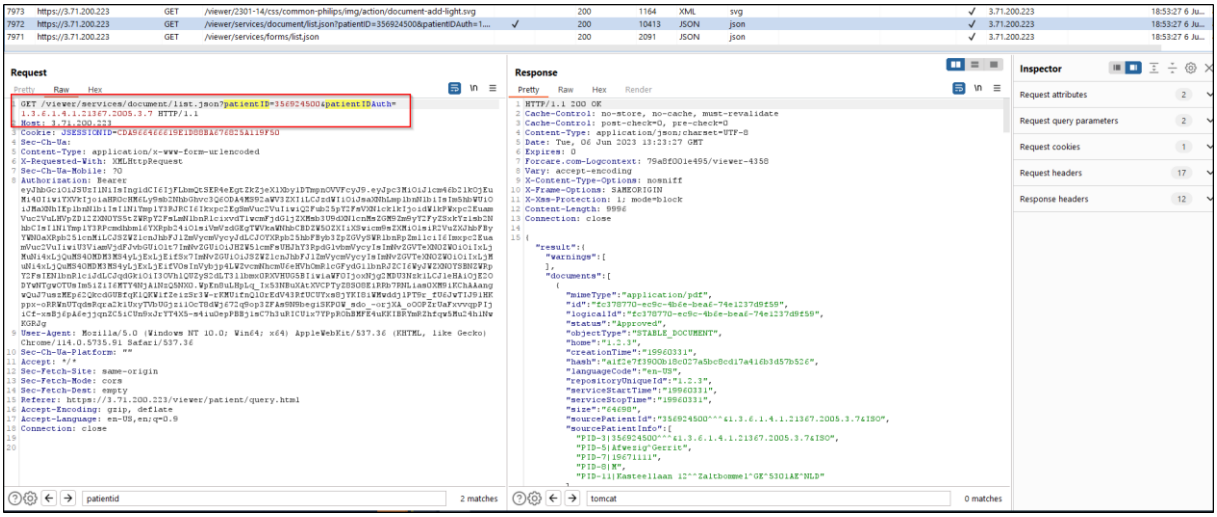


Retest (06-Jun-2023):

Steps are same as before.

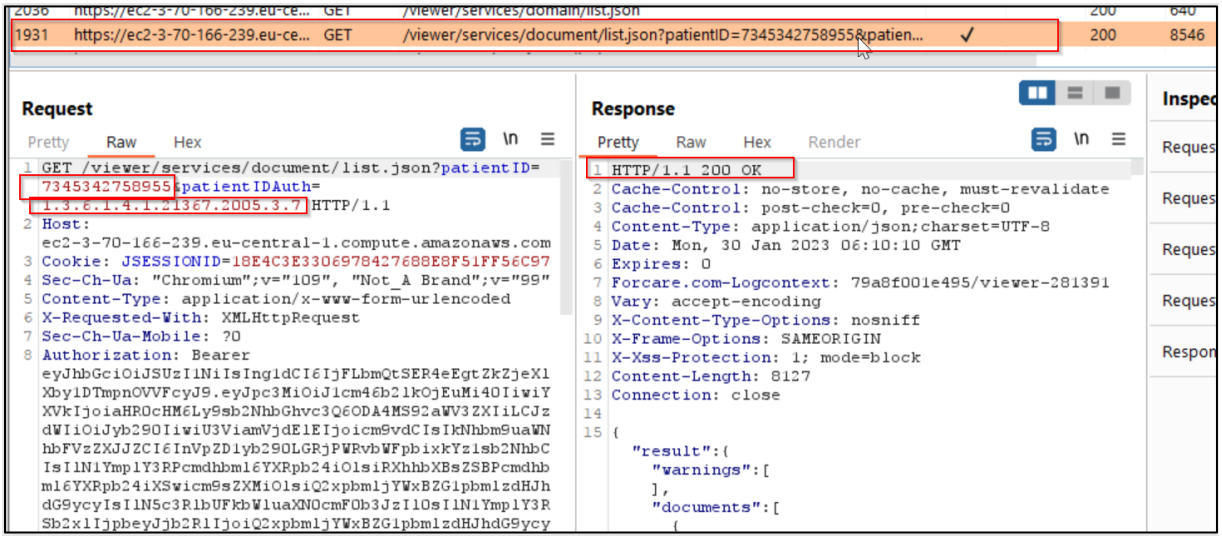
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Old POC:

- Launch ForView Applications.
- Intercept the requests using Burp proxy tool.
- As observed in below request PatientID and PatientIDAuth value gets sent for GET requests, which can get logged.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.8 Webapp: HTTP Strict Transport Security (HSTS) Not Implemented

Vulnerability Title	HTTP Strict Transport Security (HSTS) Not Implemented
Vulnerability Category	A6 - Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.8 CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L
Description	**Vulnerability Description:** The server does not implement the "HTTP Strict-Transport Security" (HSTS) web security policy mechanism. When HSTS is enabled, the web application sends a special response header, "Strict-Transport-Security" to the client with a duration of time specified. Once a supported browser receives this header, that browser can only make requests to the application over HTTPS for the duration of time specified in the header. Any links to resources over HTTP will be rewritten to HTTPS before the request is made. **Retest (23-Oct-2023):** Issue exists in Retest **Exploitability Rational:** Applications that do not utilize the "HTTP Strict-Transport Security" policy are more susceptible to man-in-the-middle attacks via SSL stripping, which occurs when an attacker transparently downgrades a victim's communication with the server from HTTPS to HTTP. Once this is accomplished, the attacker will gain the ability to view and potentially modify the victim's traffic, exposing sensitive information and gaining access to unauthorized functionality. Attacker can gain sensitive information and access for the unauthorized functionality. **Impact Rational:** Attacker can gain sensitive information and access for the unauthorized functionality.
Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload
Recommendation	The application server should send the "Strict-Transport-Security" HTTP header in each response indicating that future requests to the domain use only HTTPS. The following is a basic example of the HSTS HTTP header, setting a max-age of one year: Strict-Transport-Security: max-age=31536000 Subdomains should also be configured in this manner, by including the "includeSubDomains" flag: Strict-Transport-Security: max-age=31536000; includeSubDomains;
Status	**OPEN**

Steps to Reproduce:

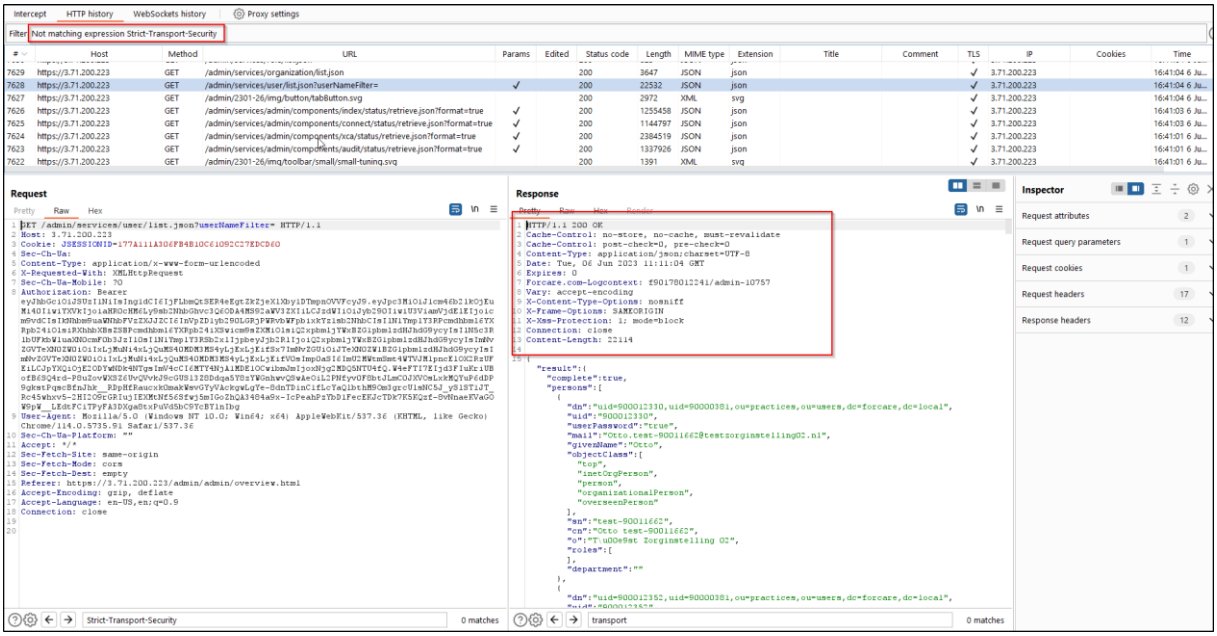
Retest (23-Oct-2023)

Supported Evidences:

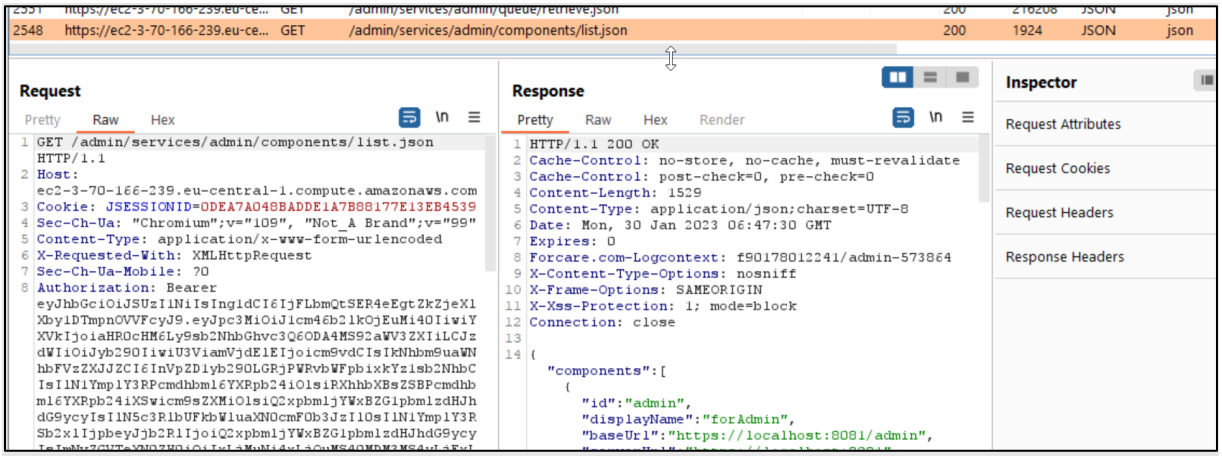
Retest (06-Jun-2023):

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Old:



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.9 Webapp: No Account Lockout Policy

Vulnerability Title	No Account Lockout Policy
Vulnerability Category	A2 - Broken Authentication
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
Description	**Vulnerability Description:** The application does not maintain or enforce an account lockout policy. A lockout policy refers to the mechanism that temporarily suspends a user's account after a certain number of unsuccessful authentication attempts have been made. **Retest (23-Oct-2023):** Issue exists in Retest. **Exploitability rational:** Applications with no lockout policy are vulnerable to brute force password guessing attacks, in which the attacker performs login attempts using a known username and a list of potential passwords until a successful combination is found. Once a successful combination is discovered, the attacker is granted full access to the compromised account and can impersonate the victim without detection. **Impact rational:** Without a strong lockout mechanism, the application can be susceptible to brute force attacks.
Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload
Recommendation	It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

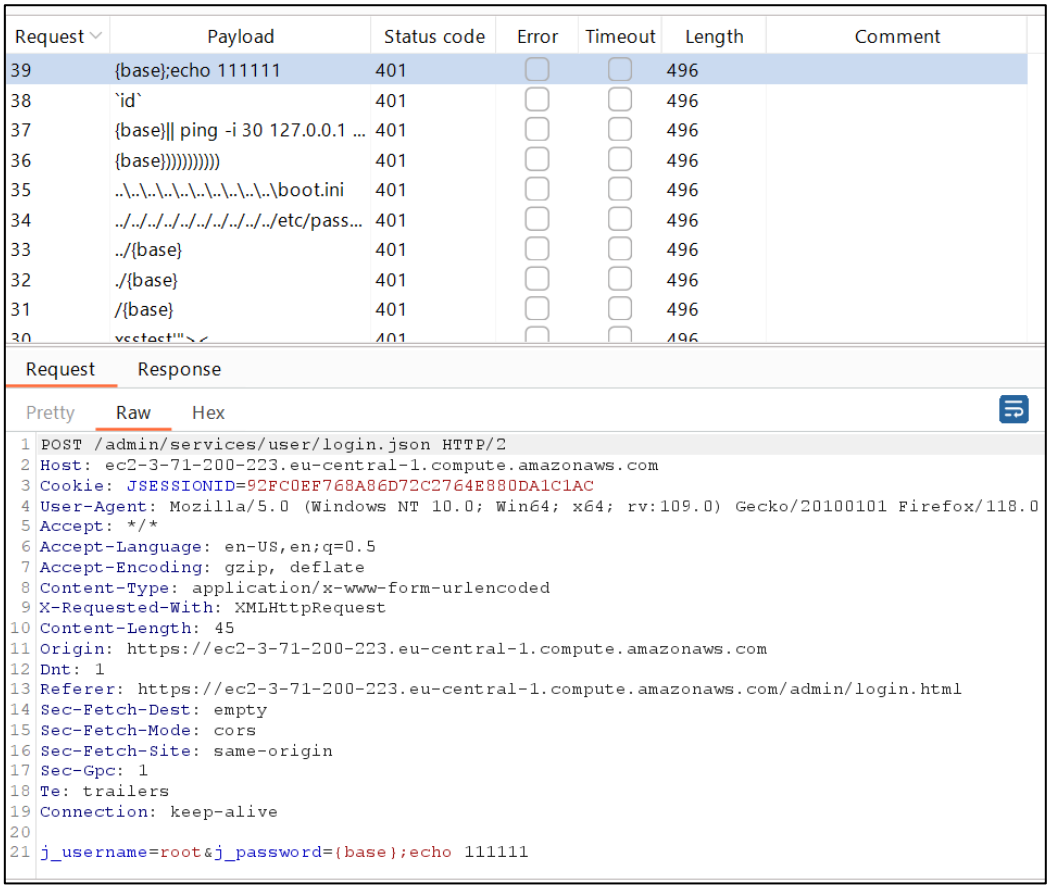
Status	OPEN

Steps to Reproduce:

Retest (23-Oct-2023):

Supported Evidences:

HTTP Request:



Request	Payload	Status code	Error	Timeout	Length	Comment
39	{base};echo 111111	401			496	
38	`id`	401			496	
37	{base}|| ping -i 30 127.0.0.1 ...	401			496	
36	{base}}}}}}}}}}	401			496	
35	..\..\..\..\..\..\..\..\..\..\boot.ini	401			496	
34	../../../../../../../../../etc/pass...	401			496	
33	../{base}	401			496	
32	./{base}	401			496	
31	/{base}	401			496	
30	xsstest"><...	401			496	

Request Response

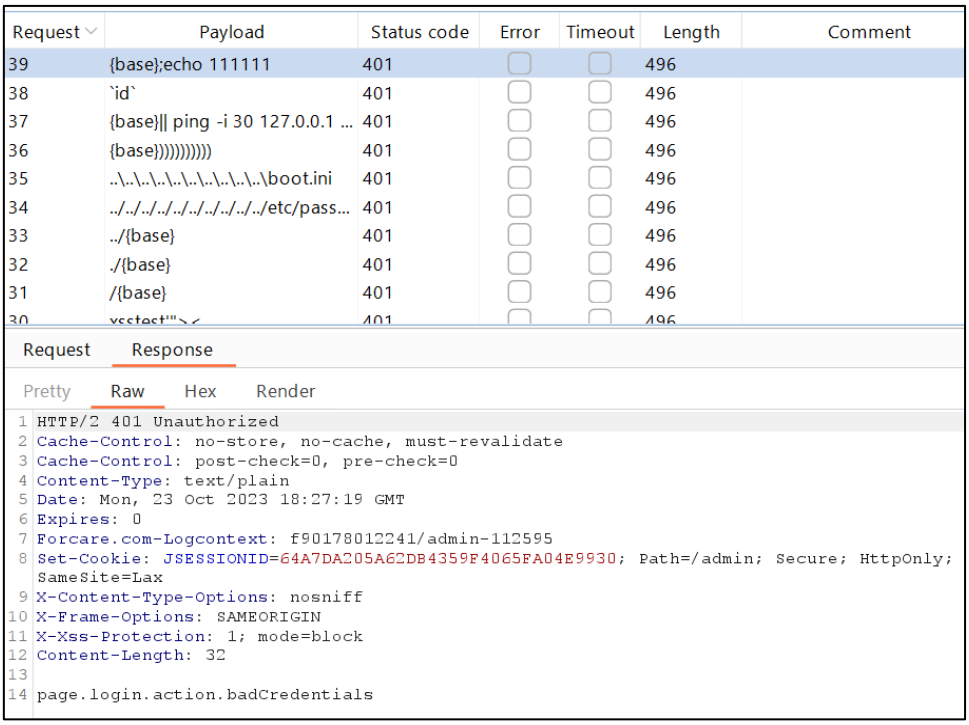
Pretty Raw Hex

```
1 POST /admin/services/user/login.json HTTP/2
2 Host: ec2-3-71-200-223.eu-central-1.compute.amazonaws.com
3 Cookie: JSESSIONID=92FC0EF768A86D72C2764E880DA1C1AC
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 45
11 Origin: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com
12 Dnt: 1
13 Referer: https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin/login.html
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17 Sec-Gpc: 1
18 Te: trailers
19 Connection: keep-alive
20
21 j_username=root&j_password={base};echo 111111
```


This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

HTTP Response:



Request	Payload	Status code	Error	Timeout	Length	Comment
39	{base};echo 111111	401			496	
38	`id`	401			496	
37	{base}|| ping -i 30 127.0.0.1 ...	401			496	
36	{base}}}}}}}}}}	401			496	
35	..\..\..\..\..\..\..\..\..\..\boot.ini	401			496	
34	../../../../../../../../../../etc/pass...	401			496	
33	.../{base}	401			496	
32	./{base}	401			496	
31	/{base}	401			496	
30	xsstest"><...	401			496	

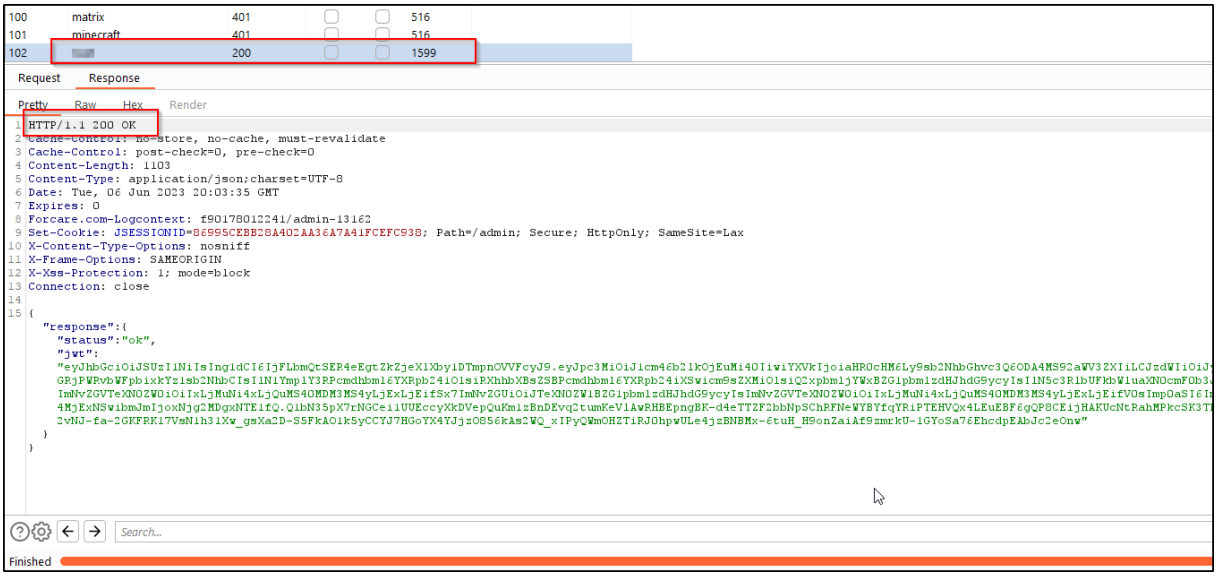
Request Response

Pretty Raw Hex Render

```
1 HTTP/2 401 Unauthorized
2 Cache-Control: no-store, no-cache, must-revalidate
3 Cache-Control: post-check=0, pre-check=0
4 Content-Type: text/plain
5 Date: Mon, 23 Oct 2023 18:27:19 GMT
6 Expires: 0
7 Forcare.com-Logcontext: f90178012241/admin-112595
8 Set-Cookie: JSESSIONID=64A7DA205A62DB4359F4065FA04E9930; Path=/admin; Secure; HttpOnly;
  SameSite=Lax
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Xss-Protection: 1; mode=block
12 Content-Length: 32
13
14 page.login.action.badCredentials
```

Retest (06-Jun-2023):

Steps are same as before.



100	matrix	401			516
101	minecraft	401			516
102	[redacted]	200			1599

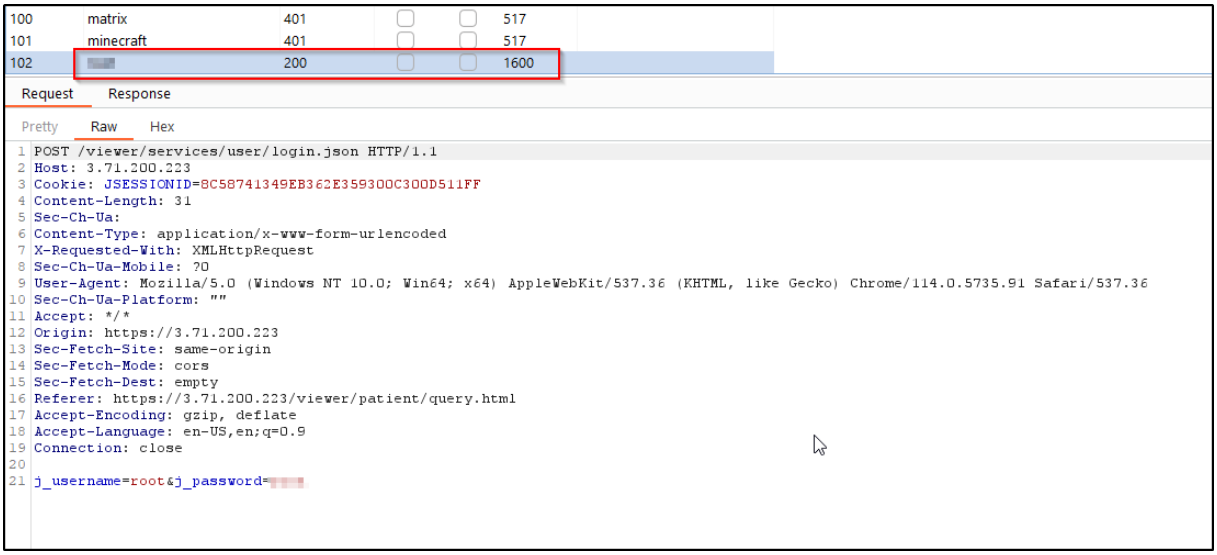
Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Cache-Control: post-check=0, pre-check=0
4 Content-Length: 1103
5 Content-Type: application/json;charset=UTF-8
6 Date: Tue, 06 Jun 2023 20:03:35 GMT
7 Expires: 0
8 Forcare.com-Logcontext: f90178012241/admin-13162
9 Set-Cookie: JSESSIONID=8E995CEBB2BA402AA36A7A41FCEFC938; Path=/admin; Secure; HttpOnly; SameSite=Lax
10 X-Content-Type-Options: nosniff
11 X-Frame-Options: SAMEORIGIN
12 X-Xss-Protection: 1; mode=block
13 Connection: close
14
15 {
    "response":{
      "status":"ok",
      "jwt":
      "eyJhbGciOiJSUzI1NiIsInglCI6IjFLbmQtSER4eEgtZkZjeXlXbylDTmpnOVVFcyJ9.eyJpc3MiOiJ1cm46b2lkOjEuMi4OIiwiYXVkIjoiaHROcHM6Ly9sb2NhbGhvc3Q6ODA4MS92aWV3ZXIiLCJzdWIiOiJ
      GRjPWRvbWFpbikxYzlsb2NhbCIsIlN1YmplY3RPcmdhbml6YXRpb24iOlsiRXhhbXBsZSBPcmdhbml6YXRpb24iXSwicm9sZXMiOlsiQ2xpbmljYWxBZG1pbmlzdHJhdG9yc
      ImNvZGVTeXNOZWOiOiIxLjMuNi4xLjQuMS40OMD3MS4yLjExLjEifSx7ImNvZGUiOiJTeXNOZWlBZG1pbmlzdHJhdG9ycyIsImNvZGVTeXNOZWOiOiIxLjMuNi4xLjQuMS40OMD3MS4yLjExLjEifV0sImp0aSI6Ik
      4MjExNSwibmJmIjoxNjg2MDgxNTE1fQ.QlbN35pX7rNGCeiIUUEccyXkDVepQuKm1zBnDEvq2tumKeVlAwRHBEpngBK-d4eTT2F2bbNpSChRFNeWYBYfqYRiPTEHVQx4LEuEBFégQP8CEijHAKUcNtRahMPkcSK3T
      2vNJ-fa-2GKFRKi7VsN1h31Xw_gsXa2D-S5FkAOik5yCCYJ7HGoYX4YJjzO856kAs2WQ_xIPyQWmOHZTiRJOhpwULe4jzBNBMx-6tuH_H9onZaiAf9zmrkU-1GYoSa76EhcdpEAbJc2eOnw"
    }
  }
```

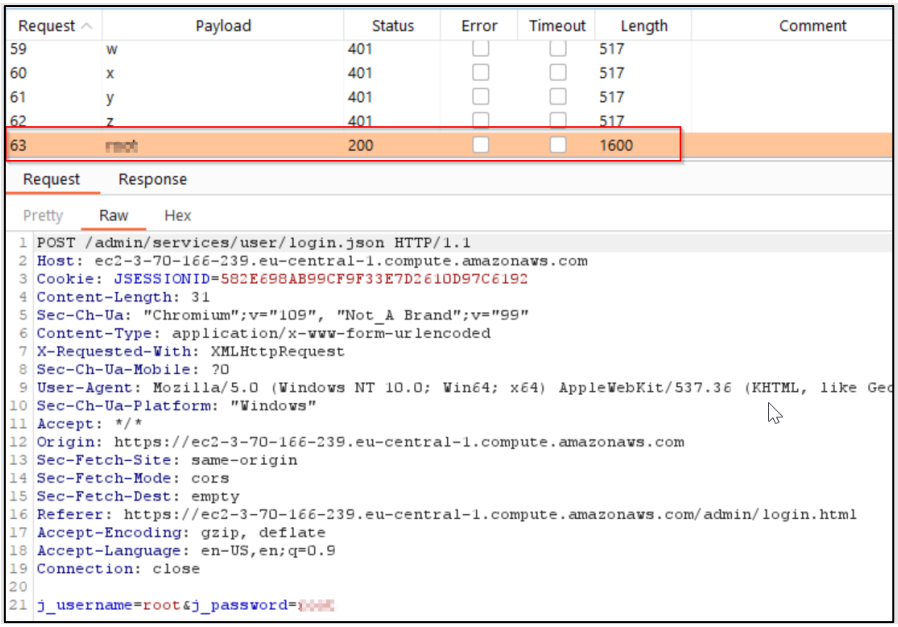

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Old POC:

- Login with username and password multiple times then you will be able to see that the account does not get locked out.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.10 Webapp: Reflected Cross-Site Scripting (XSS)

Vulnerability Category	Reflected Cross-Site Scripting (XSS)
Vulnerability Category	A3- Injection
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.5 CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N
Description	**Vulnerability Description:** A Reflected Cross-Site Scripting (XSS) vulnerability occurs when a web application sends strings that are provided by an attacker to a victim's browser in such a way that the browser executes part of the string as code. The string contains malicious data and is passed to the application through a parameter that an attacker can control (For example, a URL parameter or an HTML form field). The application immediately inserts it into its response. This results in the victim's browser executing the attacker's code within a legitimate user's session. Attackers typically exploit reflected XSS vulnerabilities by sending users malicious links containing JavaScript code (For example, via e-mail) or by posting malicious code to other sites that the vulnerable application's users may visit. **Retest (23-Oct-2023)**: Issue fixed in retest. **Exploitability rational:** Reflected Cross-Site Scripting vulnerabilities give the attacker control of the user's browser. The attack can alter page content with malicious HTML or JavaScript code. The attacker can arbitrarily alter page content displayed to the victim and can execute application functions using the victim's application identity if the victim is authenticated to the application. An often cited example use of a Reflected Cross-Site is where the attacker send themselves to the victim's session identifier. With this session identifier, the attacker can then perform application functions using that user's identity for the duration of that session. **Impact rational:** Attackers can steal cookies and change the temp look and feel using reflected cross site scripting.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer/patient/query.html#/0/document/view:medicalDocuments!patientId=7482736282%5E%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO&documentUniqueIds=079bd462-ddcb-4800-9edf-4295e3df6d54
Recommendation	Reflected Cross-Site Scripting (XSS) is prevented by encoding data before inserting it into the generated web page. Each character of the data is encoded and the result string is then inserted onto the generated web page. This technique of encoding values before inserting them on the web page is called "Output Encoding". Output encoding libraries exist for most popular programming languages and frameworks. A web page has seven different output contexts and each output context requires a different encoding scheme. Encode the data using the proper scheme. The seven different encoding schemes are: • HTML Text Element • HTML Attribute • URL Parameter • JavaScript Literal • HTML Comment • HTTP Header • CSS Property For example, the characters: <, >, ", ' are encoded as <, >, ", ' for when those characters are inserted into an HTML Text Element. When those characters are inserted as a URL Parameter, the same characters are encoded as %3C, %3E, %22, %27. Libraries for implementing the encoding schemes exist for most popular programming languages. • OWASP Java Encoder: Java only • Microsoft Web Protection Library: .NET languages • Ruby – escapeHTML() - only supports HTML Text Encoding • Jgencoder in JQuery: for preventing DOM-based XSS Green field projects can consider the use of other technologies: • Google Capabilities based JavaScript CAJA

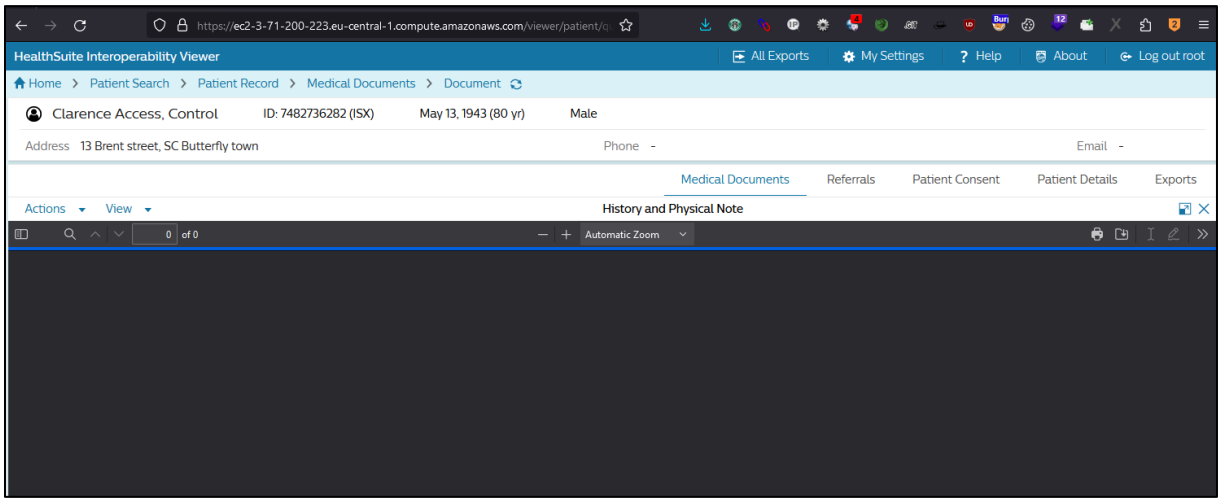
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	• OWASP JXT– automatically encodes string data with the proper encoding. Input validation is often recommended as a way to mitigate reflected cross-site scripting. It is insufficient, however, because input validation isused to prevent cross-site scripting only when the data has a strict syntactic format, such as numeric values and dates. Any application inputs which must accept arbitrary data would remain vulnerable.
Status	**CLOSED**

Steps to Reproduce:

Retest (23-Oct-2023):
Supporting Evidences:

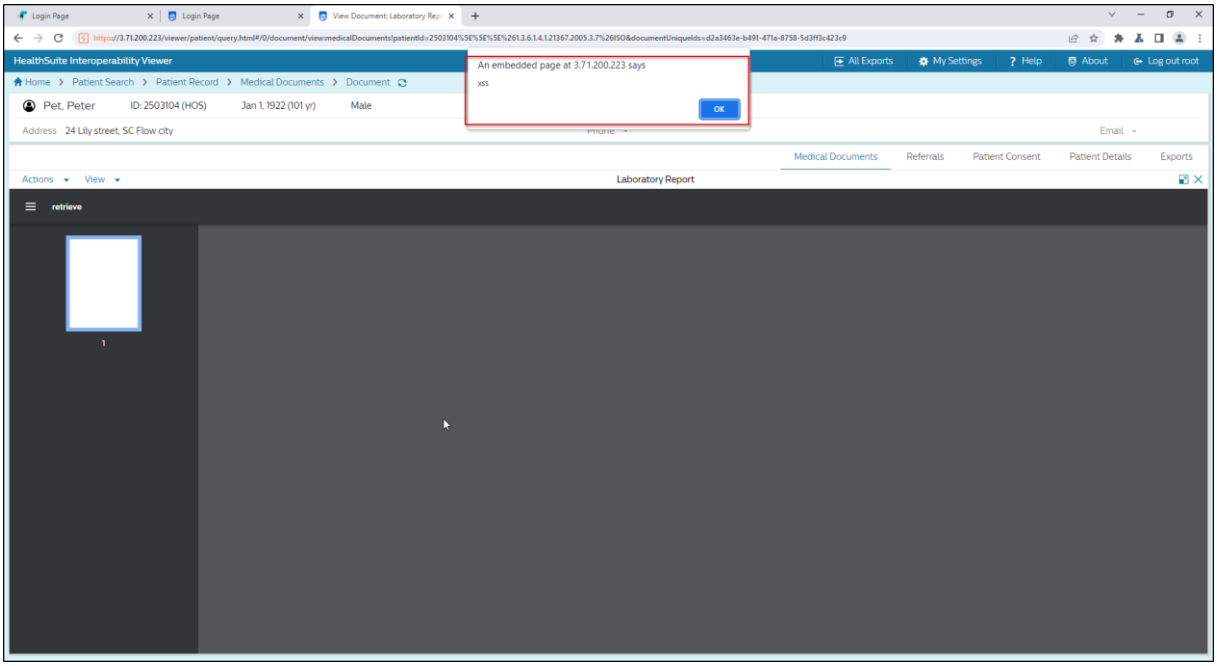


Retest (06-Jun-2023):

Steps are same as mentioned in 'Retest Status(as on 30 Jan 2023)'.

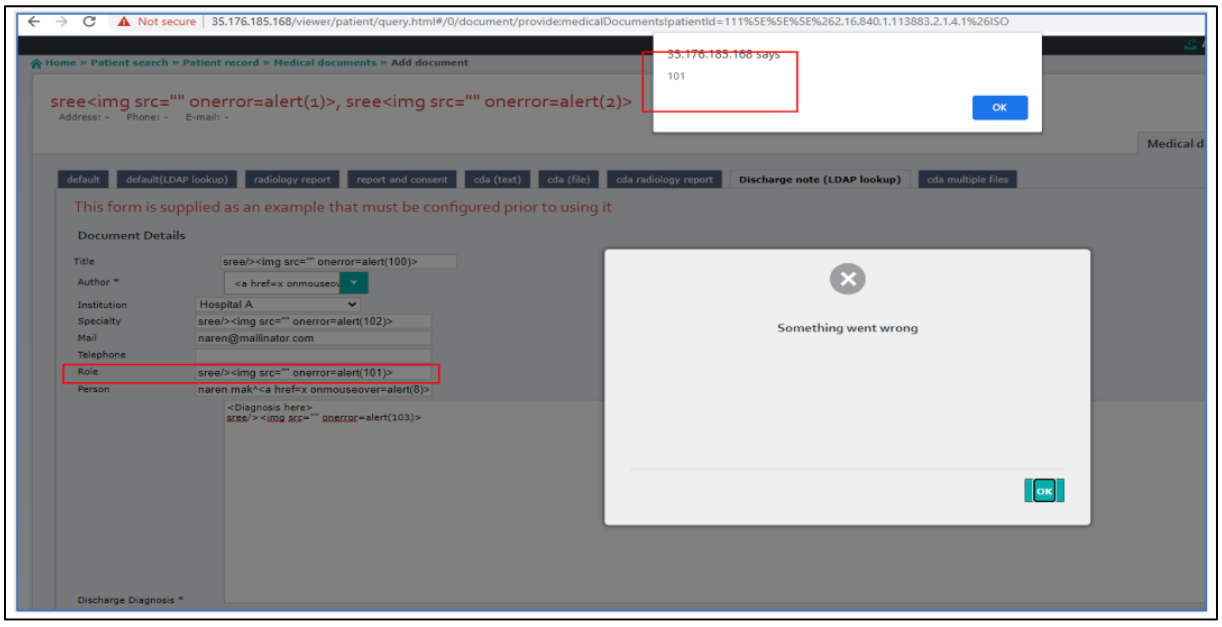
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Old POC:

Login to Viewer > Patient search >> select any patient >>> medical documents >>>> Add document >>>>> Discharge Note(Ldap lookup) >>>>>> fill the form as shown in the below snapshot and then submit, the application server responds with same malicious script without validation or encoding and execute at browser.

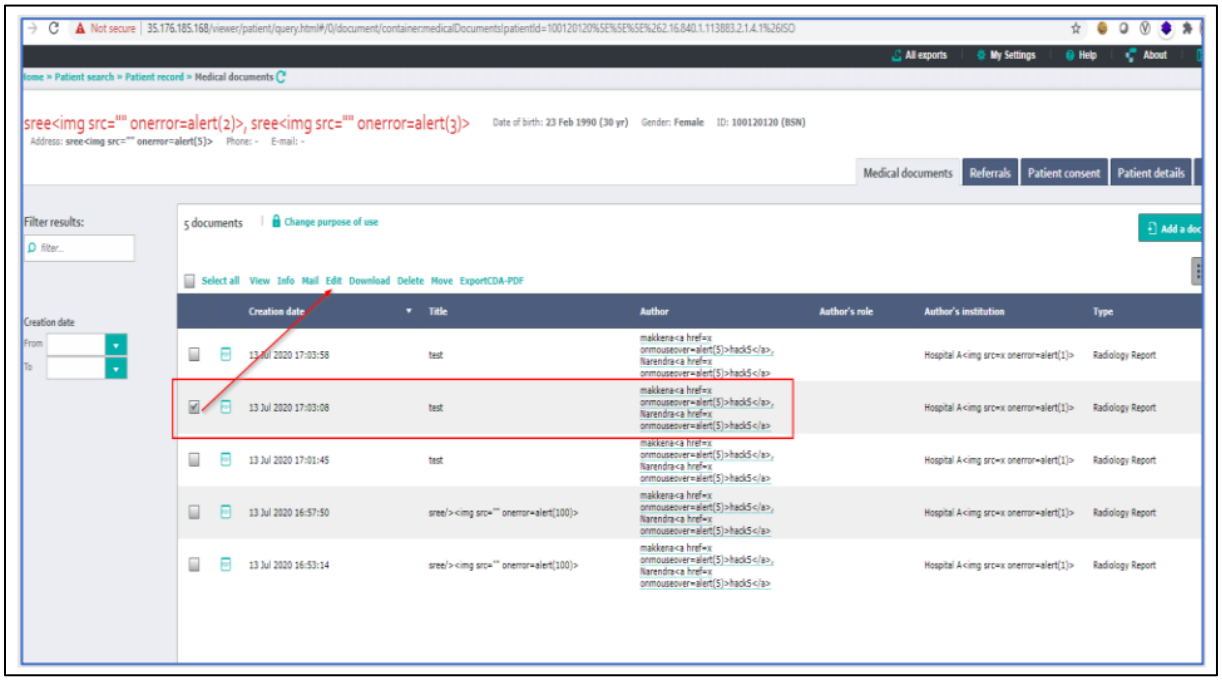


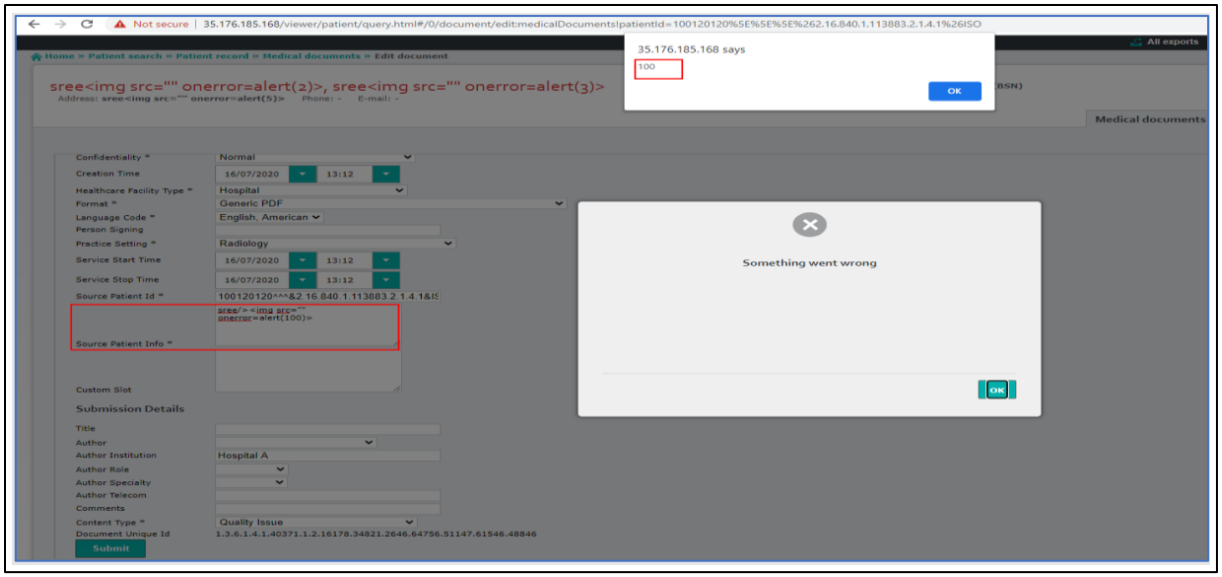
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Login to Viewer > Patient search >> select any patient >>> medical documents >>>> select any xml document >>>>> actions >>>>>> edit

Parameters: Source Patient ID & Source patient Info





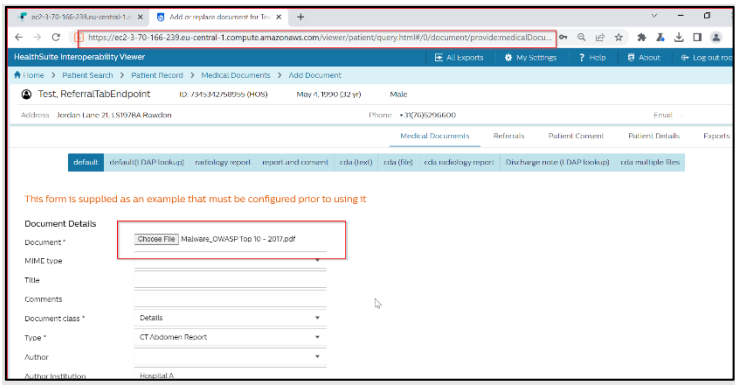
Retest Status(as on 30 Jan 2023)

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

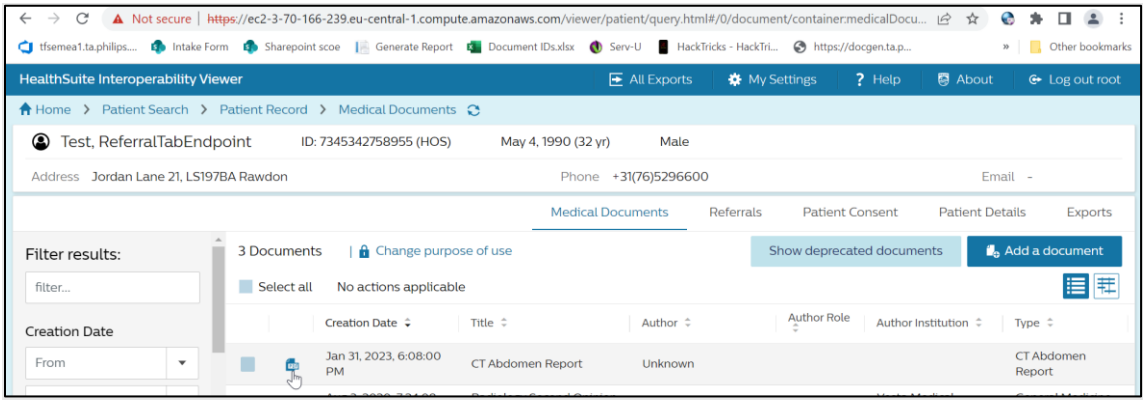
Printed copies are uncontrolled unless authenticated.

Issue still persists.

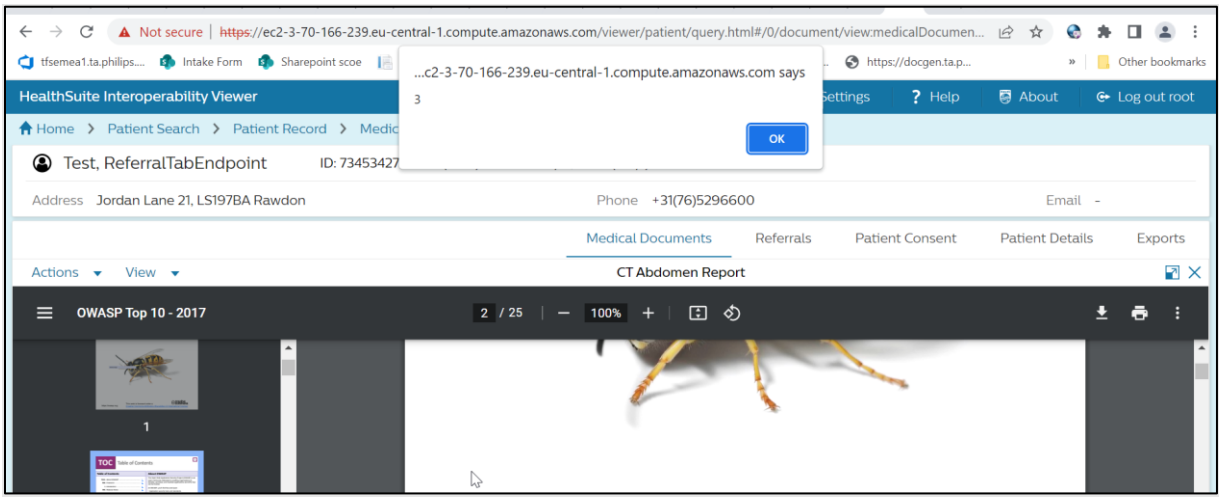
Uploading a pdf which has malicious script.



- Upload the file and navigate to Medical Documents section.
- Click the pdf icon for the patient where the document is upload.



- Scroll the launched pdf and you can see the JavaScript getting executed.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.11 Webapp: Weak SSL/TLS Configuration

Vulnerability Title	Weak SSL/TLS Configuration
Vulnerability Category	A2 Cryptographic Failures
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** It is observed that the server-side SSL/TLS endpoint is configured to allow weak SSL/TLS cipher suites in the provided server. TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) **Retest (23-Oct-2023):** Issue exists in Retest. **Exploitability Rational:** Some misconfiguration in the server can be used to force the use of a weak cipher - or at worst no encryption - permitting to an attacker to gain access to the supposed secure communication channel. Other misconfiguration can be used for a Denial-of-Service attack. **Impact Rational:** A server-side SSL/TLS endpoint that supports weak ciphers can allow an attacker to read or modify traffic sent in SSL/TLS connections with that endpoint.
Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com
Recommendation	Update the server-side TLS endpoint's configuration to allow only TLSv1.2 or TLSv1.3 connections with cipher suites that use the following: • Ephemeral Diffie-Hellman for key exchange (Optionally, allow RSA for key exchange if necessary for supporting some clients).

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	• Block ciphers in GCM mode. Note: If CBC mode must be allowed for supporting some clients, use only CBC mode cipher suites that use the SHA2 family of hash functions (SHA256, SHA384, SHA512).
Status	**OPEN**

Steps to Reproduce:

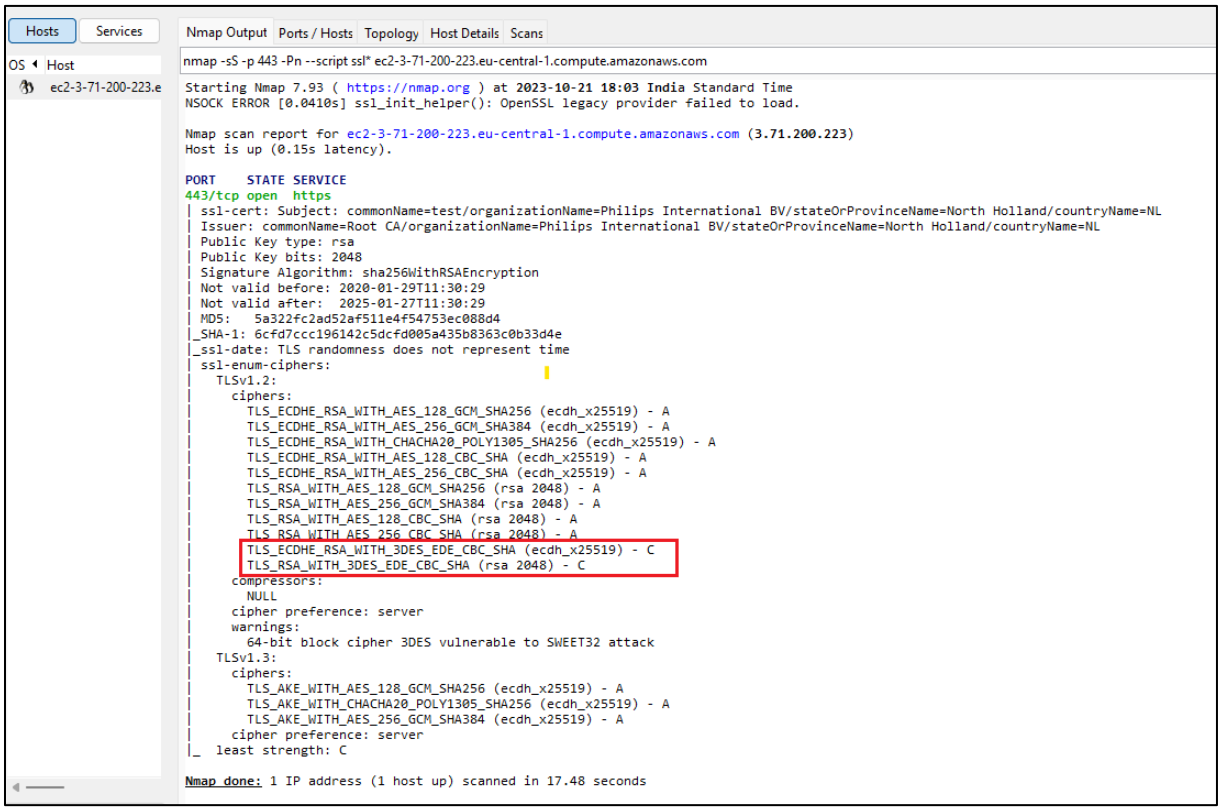
Retest (23-Oct-2023):

Supported Evidences:

```
Testing SSL server ec2-3-71-200-223.eu-central-1.compute.amazonaws.com on port 443 using SNI name ec2-3-71-200-223.eu-central-1.compute.amazonaws.com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.3  128 bits  TLS_AES_128_GCM_SHA256        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_CHACHA20_POLY1305_SHA256  Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_AES_256_GCM_SHA384        Curve 25519 DHE 253
Preferred TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-CHACHA20-POLY1305   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  112 bits  ECDHE-RSA-DES-CBC3-SHA        Curve 25519 DHE 253
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA
```


This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

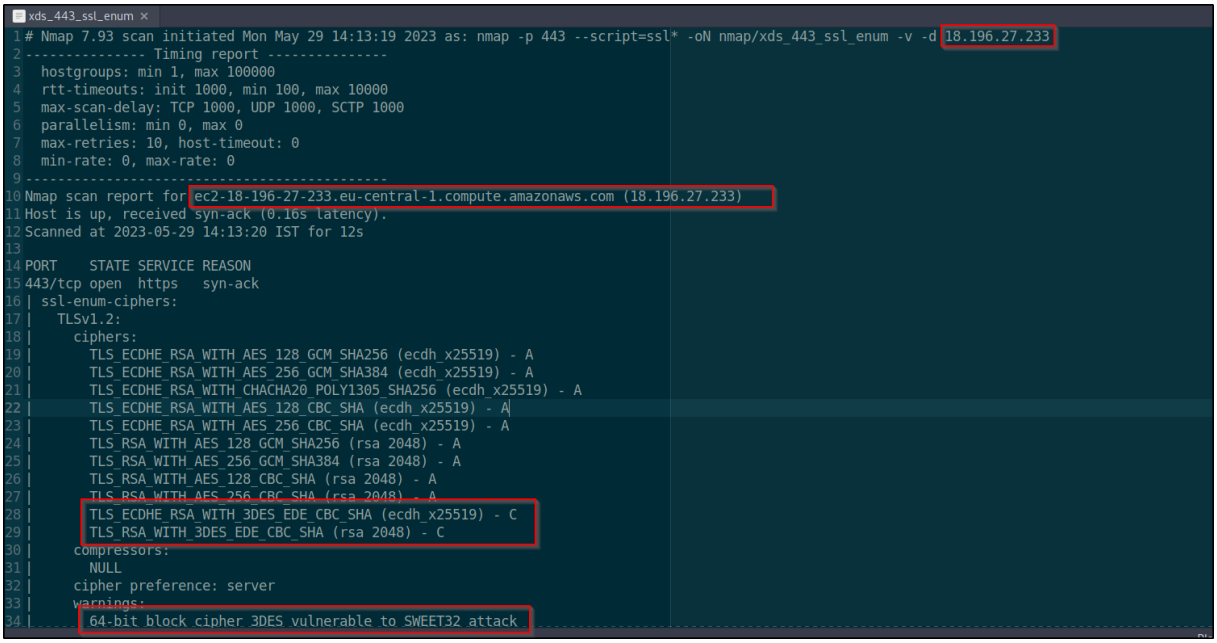


Retest (06-Jun-2023):

Steps are same as before.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Old POC:

Use Nmap to enumerate the ciphers used by the application endpoints.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-23 18:30 India Standard Time
Nmap scan report for ec2-3-70-166-239.eu-central-1.compute.amazonaws.com (3.70.166.239)
Host is up (0.14s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (ecdh_x25519) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|     cipher preference: server
|_  least strength: C

Nmap done: 1 IP address (1 host up) scanned in 12.22 seconds
```


This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.12 Webapp: Missing Security Header

Vulnerability Title	Missing Security Header
Vulnerability Category	A5 Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.9 CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:L
Description	**Vulnerability Description:** During security assessment, we found that either the security headers are not configured properly, or security headers are missing in response. Security headers in the response can be used to increase the security of the application. The missing security headers are: • Content-Security-Policy **Exploitability Rational:** Exploitability of these depends differently based on the missing headers. Like Cache-Control headers require physical access to the system. But others require user interaction to exploit this vulnerability. **Impact Rational:** These headers provide the additional security at client side. Missing these headers may lead to sensitive information disclosure like account take over etc.
Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload/?assigningAuthority=1.3.6.1.4.1.21367.2005.3.7#/start
Recommendation	It is recommended to configure all the security headers in the response to improve your application's security.

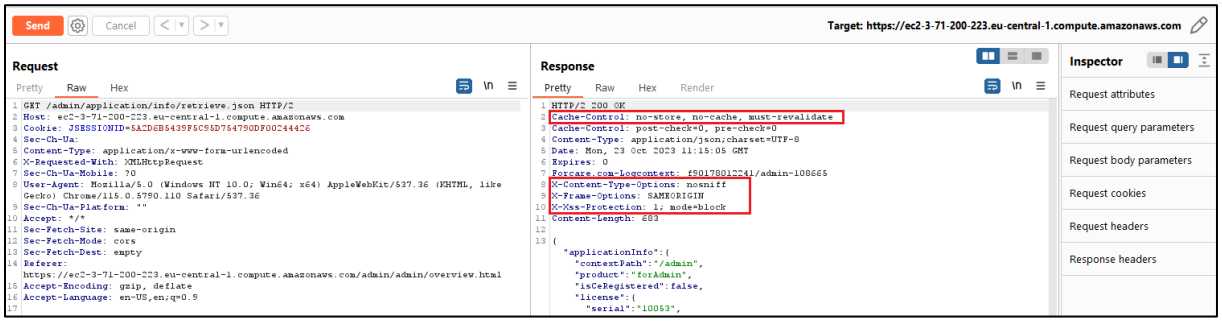
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Status	OPEN

Steps to Reproduce:

Supportive Evidences:



CSP not set

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8.13 Webapp: Server Banner Disclosure

Vulnerability Title	Server Banner Disclosure
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** During the security assessment, it was found that the application discloses the application server details including the version in the HTTP response. Targeted attacks can be launched against the server based on the exploits it is having. **Exploitability Rational:** Web server fingerprinting is a critical task for the penetration tester. Knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing and those are available on internet. **Impact Rational:** Targeted attacks can be launched against the server based on the exploits it is having.
Affected Systems/IP Address/URL	https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin
Recommendation	It is recommended to use custom banner for server by hiding all sensitive information from banner.
Status	**OPEN**

Steps to Reproduce:

Supported Evidences:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Apache Tomcat/9.0.71

Apache Tomcat/9.0.71

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

9. Tools Used

Scope	Tools Used
Web Application Security	Burpsuite pro, nmap

10. Automated Tool Report

NA

11. Manual Test Reports and Test Case Execution

Testsuite_WebApp.xlsx

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.